From: OFFICER Magazine
To: LaLiberte, Chad (POL)
Subject: A Data=Driven Approach | Radar Speed Signs | ALPR | Learning the Hard Way
Date: Friday, March 24, 2023 10:15:47 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.

Officer Magazine eNL | View online

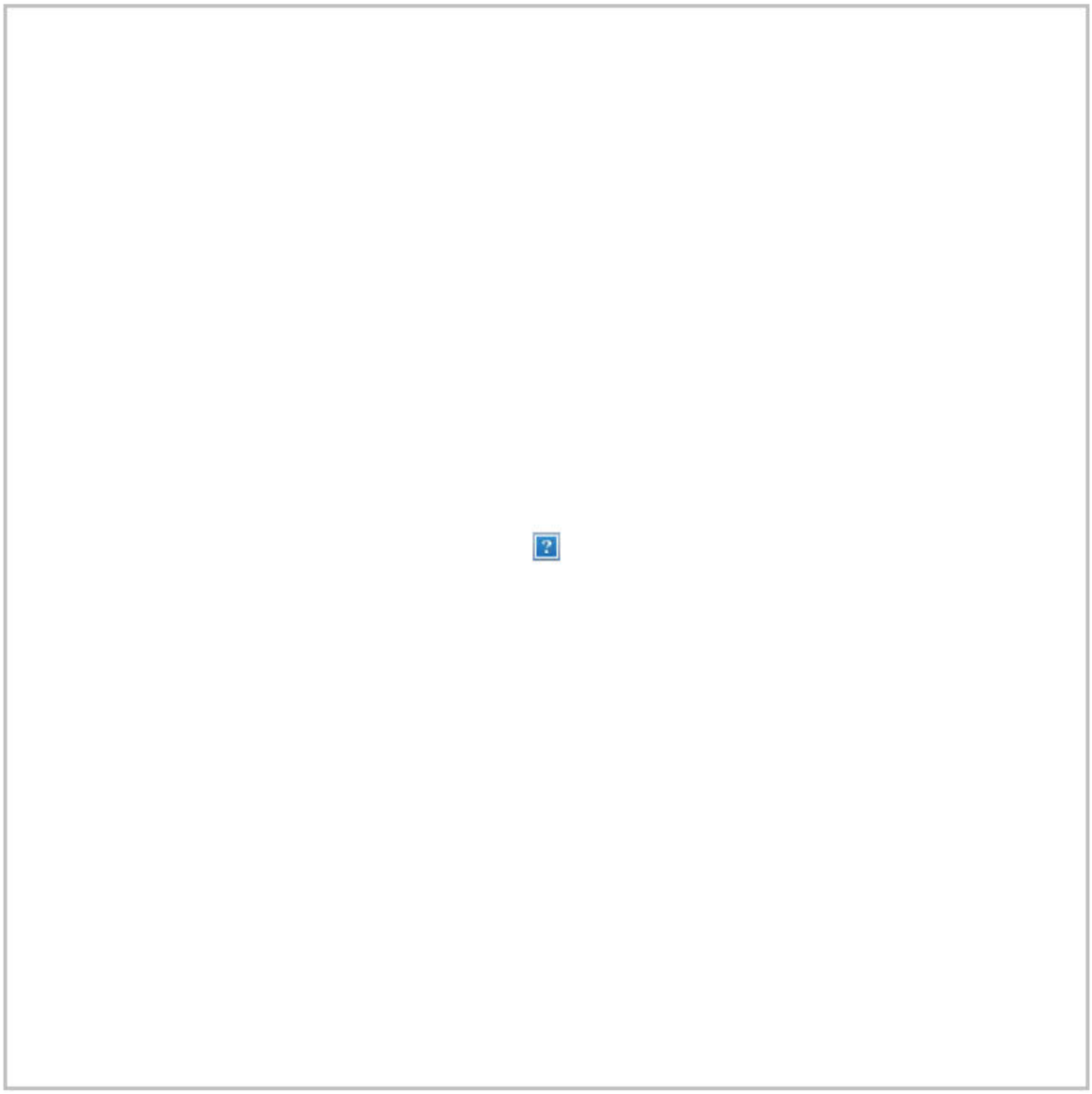
officer.com header logo

COVER STORY

A Data-Driven Approach to Traffic Safety

Online cloud-based crash reporting solutions allow for better data access and analytics.

IN THIS ISSUE



Radar Speed Signs: A Small Solution to a Big Problem

Radar speed signs can help slow down traffic without taking up valuable manpower.



Keeping an Eye on Traffic with Automatic License Plate Readers

Automatic License Plate Readers (ALPR) can do much more than just capture numbers and letters on a plate.



Calling All Cars: Have Police Vehicle Supply Chain Issues Improved?

A global microchip shortage and supply chain issues caused delays on getting new vehicles to departments in 2022. Will 2023 be any better?

Learning the Hard

Glock 29SF



Way: Keeping Use-of-Force Training Safe

Tragedy struck three law enforcement training exercises late last year. Instructors discuss the lengths they go to for safety and how accidents can be prevented.



The Right Shield for the Job

Manufacturers have worked to create single-handed ballistic shields that can be used during active shooter incidents.



The Absurdities of the Job: Managing New Recruits' Expectations

New recruits to law enforcement agencies can come with unrealistic expectations, and it's up to departments to prepare them for the realities of the job ahead of them.



Review: Gun to Have Against a Charging Target

Despite the power of the 10mm cartridge, the Glock 29SF was easy to handle, comfortable to shoot and delivered accurate fire.



The Blurring of Body Armor vs Tactical Wear

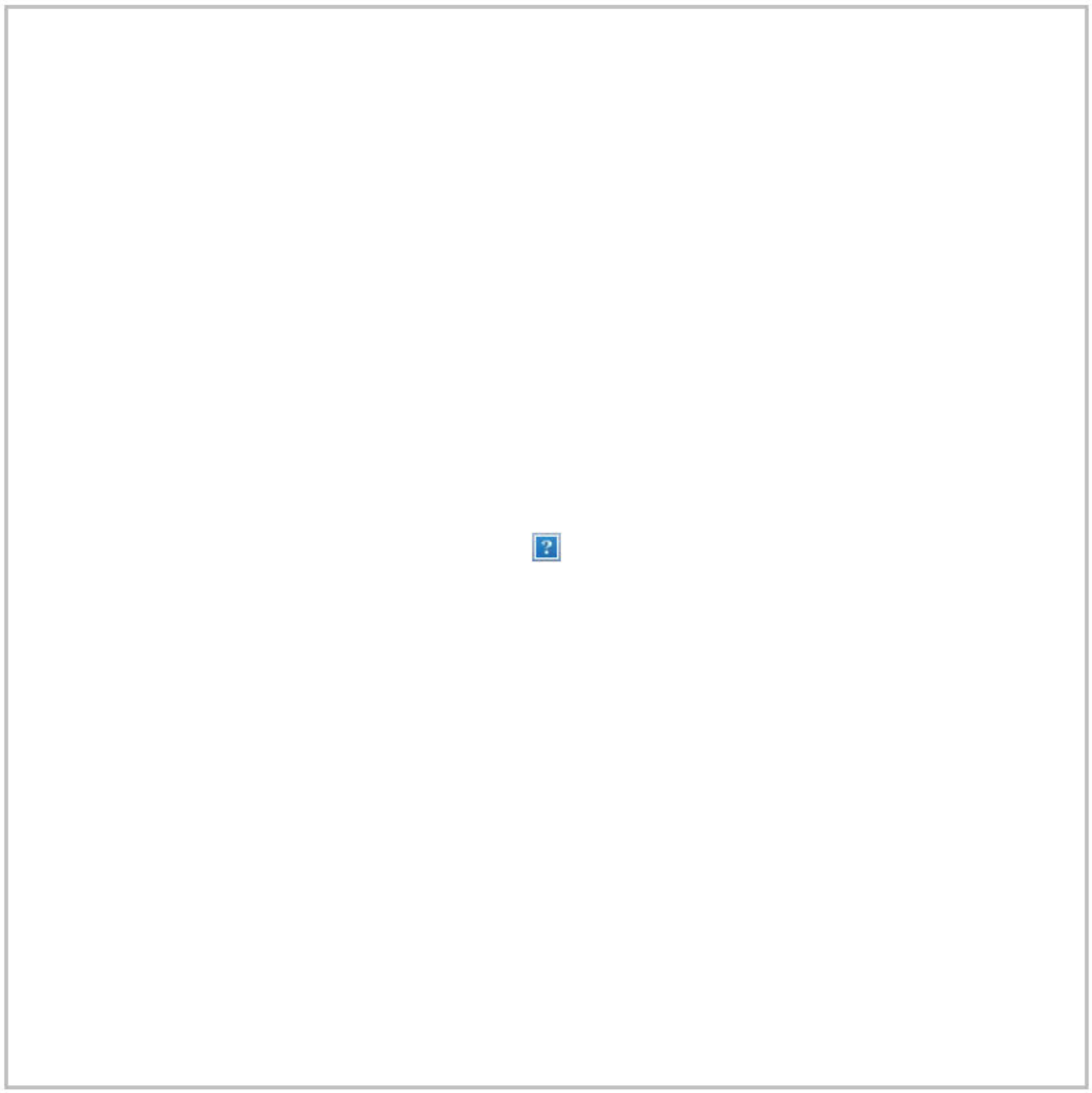
A look at how body armor carriers have evolved to be more comfortable and healthier for the officers working 10-plus hour shifts.



How to Catch A Criminal: A Messy Separation Part I

This month, how a wife's scheme tears her marriage apart, literally.

NEW PRODUCTS



Vanguard Level III
From Point Blank Enterprises Inc.

The Vanguard from Point Blank Enterprises provides level III rifle threat protection and is available in three shapes. A wide rectangular shaped viewport provides excellent viewing capabilities while the weapon index platform on each side allows the operator to position their weapon for accurate handgun or long-gun deployment.Learn more about one o...

Origin System by PARACLETE
From Point Blank Enterprises Inc.

The Origin System by PARACLETE from Point Blank Enterprises builds upon the developing needs of military and law enforcement service members. It applies technology in new innovative ways to reduce bulk, maximize adaptability, improve strength and durability and allow users to change mission load outs as often as threat levels do, in ways that surpa...

T8 Extreme 200G Thinsulate
From Garmont Tactical

The T8 Extreme 200G Thinsulate boots from Garmont Tactical are designed to meet current U.S. Army and Air Force standards, this version of our Extreme features a 200g 3M Thinsulate® membrane that makes it the ideal choice for windy days or very harsh climates. This style is also durable, thanks to its strong anti-abrasion materials combining leathe...

LEOLITE Transport
From KIMTEK Corporation

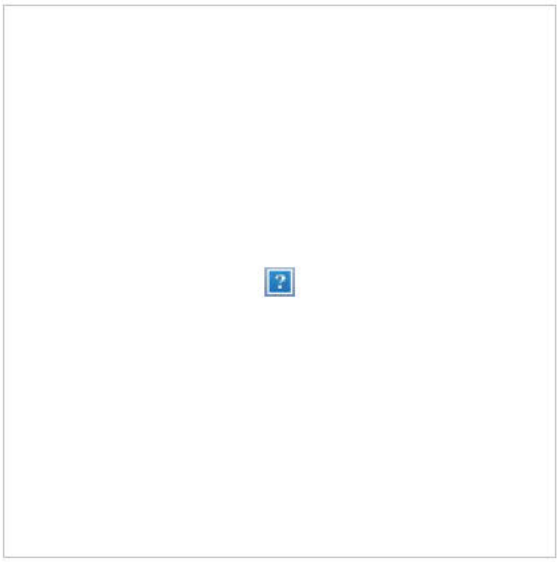
The LEOLITE Transport LEO-501 from the KIMTEK Corporation is designed to carry two officers on two seats with seat belts. The two seats are easily and quickly locked in and out utilizing our unique quick lock

ASP Integrated Training
From ASP Inc.

ASP Integrated Training (Tactical Baton, Restraint and Performance Flashlight) puts no principle above simplicity. Techniques are simple to learn, easy to understand, effortless to remember, and designed to

release mechanism with no tools required.Each LEOLITE comes with a full base with lockable storage box for weapons and ammunition. A stainles...

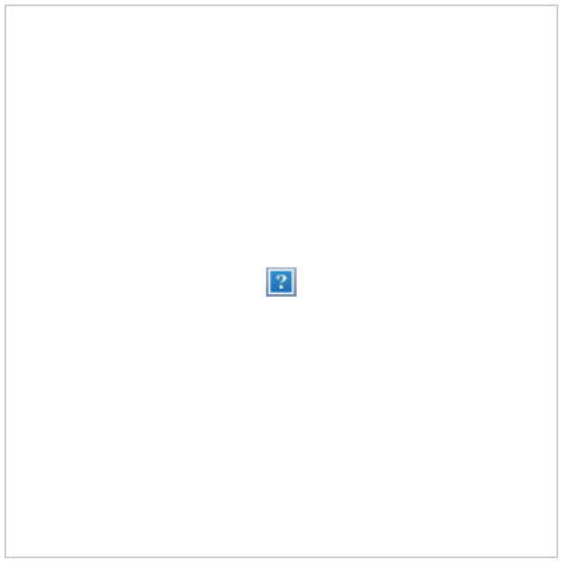
work for all officers, not just those highly skilled in psychomotor performance. ASP techniques work on the street, not just in the ideal envir...



Magnet OUTRIDER: Perform lightning fast scans for digital contraband on-scene

From Magnet Forensics Inc.

Magnet OUTRIDER is a triage tool that enables officers and digital forensics professionals to rapidly scan computers and storage devices on-scene and in the lab to determine whether they contain child sexual abuse material or other illicit content.When officers arrive on-scene, time is of the essence. Agencies will often find multiple devices in a ...



ShotSpotter Investigate

From ShotSpotter

ShotSpotter Investigate is a leading case management solution that helps law enforcement agencies achieve higher clearance rates, especially for violent crimes. The cloud-based system enables agencies to better capture, track, analyze and collaborate on investigations enabling them to be more efficient and effective. The system creates a single, se...

READ THE LATEST DIGITAL EDITION



Read the Officer Magazine January/February 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

This email is being sent to chad.w.laliberte@state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: Pack, Noah (POL)
To: ALPR_Support; mroth; Israel Padilla
Cc: Walczak, Ryan (POL)
Subject: ALPR Read Time Verification
Date: Wednesday, November 8, 2023 1:26:50 PM

Hi Israel and team:

Prior to the system shut down in 2020, we understand that the system upload time for all reads in the system at the time of the shut down was preserved. We've been asked to assist with introducing a read in court from that time period, and we would like to check the system upload time for that read. Are you still able to access and check that data? We are told it was held by Neology.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

From: Genetec newsletter
To: Haywood, Antwan (POL)
Subject: Antwan, see why IIoT matters
Date: Thursday, July 27, 2023 1:02:11 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.

Connecting the dots from Genetec

Hi Antwan,

Everything you ever wanted to know about the Industrial Internet of Things (IIoT) is here! We even included real-life customer examples to give you ideas about how your team can connect IIoT sensors to get more from your physical security system.

Happy reading,

Julie Cadieux, **Senior Editor**
jcadieux@genetec.com

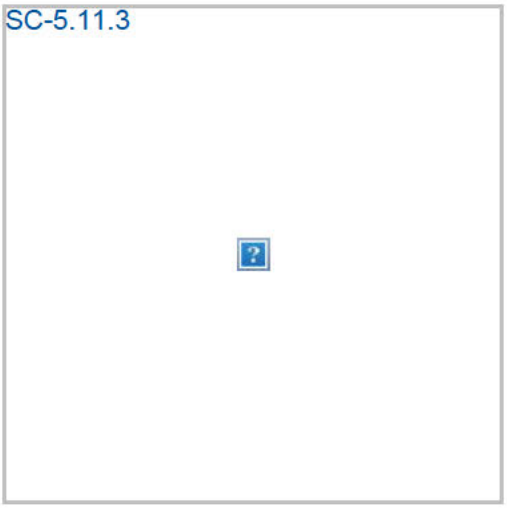
Product updates

Security Center 5.11.3

The latest release simplifies password management, allows you to schedule automatic firmware updates, and create dashboard customizations.

Read →

SC-5.11.3



SIP-mobile



Take SIP calls on the go

The new version of Sipelia™ turns your mobile phone or tablet into a powerful security communication device.

← Read

Want better ALPR capture rates?

AutoVu™ Sharp Z3, our ALPR solution, has major new features

like stereoscopy, analytics, and dual exposure.

Read →

ALPR-AutoVu

Industrial Internet of Things

IoT-IIoT

Why IIoT matters

Find out how cloud, cybersecurity, unification, and AI impact the success of your IIoT journey.

← Read

Tips & tricks

TechDoc Hub

Check out the Genetec™ Mobile Getting Started Guide to learn how to perform Security Desk monitoring functions from your smartphone.

Read →

Genetec-mobile

people-detection

How does YOLO work?

Learn about object detection in video analytics, and why everyone's talking about the YOLO algorithm.

← Read

ClearID

Looking for ways to ensure security compliance and audit readiness?

Discover a simplified auditing process that allows you to schedule or manually launch access reviews through a self-service portal.

Simplify the audit process with ClearID

Get the updates you need

Select products of interest, preferred language, and more in our email preference center.

Manage your preferences →

View this online · Manage your preferences · Unsubscribe

Genetec Inc.
2280 Alfred-Nobel Blvd., Montreal, QC H4S 2A4 Canada

© 2023 Genetec Inc. TM trademark of Genetec Inc.

From: John Tedona
To: Pack, Noah (POL)
Subject: Automatic reply: Total data counter reduction, possible data deletion.
Date: Wednesday, September 20, 2023 6:26:47 PM

Hello,

Thank You for your email. I am currently out of the office until Monday, September 25th. with limited access to email. If you require immediate assistance for ALPR products please contact Customer Support at Alpr_support@neology.net or (833)-747-7577

Thank You

John Tedona

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Bill: Drop LEO hiring age to 18; Cop charged in teen"s death had PD reprimands
Date: Monday, March 6, 2023 5:38:28 PM

March 6, 2023 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

You have until midnight to share the impact of police staffing issues at your agency for Police1's "What Cops Want in 2023" survey. Don't miss the opportunity to make your voice heard. Your answers will provide law enforcement leaders and elected officials insight into how short staffing is directly impacting your safety and wellness.

Click here to take the survey.

Stay safe,

— The Police1 Team

TOP STORIES

Rocks, bricks, Molotov cocktails, fireworks thrown at cops at Atlanta training center site

Some 35 people had been detained as other police agencies stepped in to assist the city's officers

Fired Memphis FD EMT says police impeded Tyre Nichols' care

Off-duty officer helps rescue boy hanging by the neck at Pa. amusement park

Ohio bill may drop minimum LEO hiring age from 21 to 18 to help recruitment

Ex-cop in teen's death faces new charge, report highlights PD reprimands

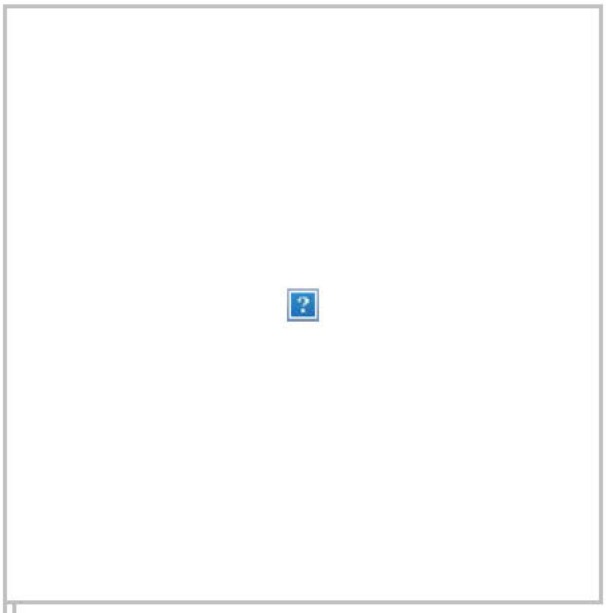
Traffic stop leads to lifesaving brain tumor surgery for S.C. woman

Manage digital investigations in one place.



Law Enforcement Media Analysis identifies and extracts facts from video and image evidence during investigations.

Request a demo



POLICE INVESTIGATIONS



Amateur websleuth groups: A rapidly evolving risk for police

By Ted Bremer

Supervisors need to continually remind their officers about operational security, so all information stays in the hands of investigators



‘Catch me if you can!’ Criminal interrogation tactics for the narcissist

By Louis C. Senese

Would a narcissist ever waive their Miranda rights and allow law enforcement to question them regarding a crime? Some will because of ego

Effectively leveraging mobile technology



Join us to hear recommendations on full mobile deployment to your organizations

Register for the webinar - Thursday, March 9 (3pm ET)

DOMESTIC VIOLENCE CALLS

What are the predictors of staged suicide scenes in domestic violence cases?

By David Cropp

The most common victim-offender relationship involving homicide scene staging is an intimate partner relationship

Report details how one police department addresses domestic-related repeat calls for service

By David Cropp

Sergeants must play a key role in domestic violence-related responses – not just for repeat calls for service but also in managing high-risk calls

SPONSORED CONTENT

Why Neology is an ALPR partner you can rely on

Police departments need an ALPR like the Neology Helios, which features powerful on-camera processing that provides immediate results.

FEATURED JOB

Alaska State Trooper Entry/Lateral ($10,000 Move Reimbursement)
Anchorage, AK
Entry Level: $37.13 hourly

FEATURED JOB

Police Officer - $25,000 Lateral Hiring Incentive
Federal Way, Washington
$6,330 - $8,492 month
(Effective. Jan 1, 2023)

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 © 2023 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Genetec newsletter
To: zzEgnitz, Brian (POL)
Subject: Brian, see why IIoT matters
Date: Thursday, July 27, 2023 1:02:47 PM

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

Connecting the dots from Genetec

Hi Brian,

Everything you ever wanted to know about the Industrial Internet of Things (IIoT) is here! We even included real-life customer examples to give you ideas about how your team can connect IIoT sensors to get more from your physical security system.

Happy reading,

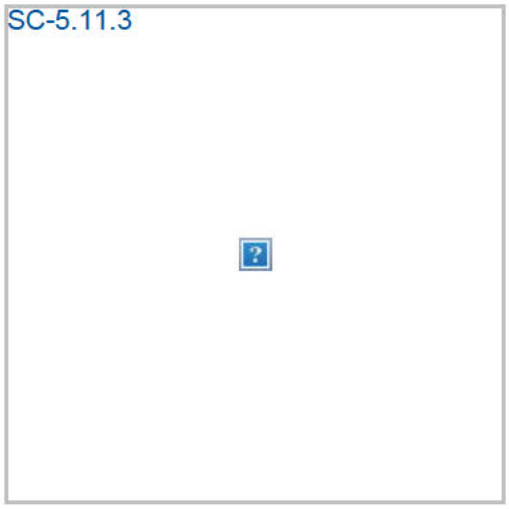
Julie Cadieux, **Senior Editor**
jcadieux@genetec.com

Product updates

Security Center 5.11.3

The latest release simplifies password management, allows you to schedule automatic firmware updates, and create dashboard customizations.

Read →





Take SIP calls on the go

The new version of Sipelia™ turns your mobile phone or tablet into a powerful security communication device.

← Read

Want better ALPR capture rates?

AutoVu™ Sharp Z3, our ALPR solution, has major new features

like stereoscopy, analytics, and dual exposure.

Read →

ALPR-AutoVu

Industrial Internet of Things

IoT-IIoT

Why IIoT matters

Find out how cloud, cybersecurity, unification, and AI impact the success of your IIoT journey.

← Read

Tips & tricks

TechDoc Hub

Check out the Genetec™ Mobile Getting Started Guide to learn how to perform Security Desk monitoring functions from your smartphone.

Read →

Genetec-mobile

people-detection

How does YOLO work?

Learn about object detection in video analytics, and why everyone's talking about the YOLO algorithm.

← Read

ClearID

Looking for ways to ensure security compliance and audit readiness?

Discover a simplified auditing process that allows you to schedule or manually launch access reviews through a self-service portal.

Simplify the audit process with ClearID

Get the updates you need

.ıail icon

Select products of interest, preferred language, and more in our email preference center.

Manage your preferences →

View this online · Manage your preferences · Unsubscribe

Genetec Inc.
2280 Alfred-Nobel Blvd., Montreal, QC H4S 2A4 Canada

© 2023 Genetec Inc. TM trademark of Genetec Inc.

From: Police1 Weekend Roll Call
To: McCarthy, Steven (POL)
Subject: BWC of "deeply disturbing" shooting that killed LEO & other top stories
Date: Sunday, June 11, 2023 8:04:15 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.

FEATURED CONTENT



Colo. officer shot multiple times while sitting in patrol vehicle

The suspect approached the officer and opened fire; the officer was hit, yet managed to exit his vehicle, take cover and return fire



Bodycam: LAPD stop knife-wielding man who attacked Metro passengers

The suspect had already stabbed a man before LAPD located him in a parking lot



'Deeply disturbing' bodycam video shows shooting that killed Calif. officer

The suspect's first shot hit and killed Det. Benedetti; the suspect took Benedetti's rifle and fired additional shots, striking another officer

Be ready for today's law enforcement technology while preparing for tomorrow

In this free webinar, learn how to assess and prepare your agency's bandwidth for

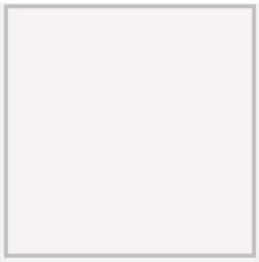
Making informed decisions on new technology

Join us to learn about key considerations for adopting new police technology.



ever-evolving technology.

Register for the webinar - Thursday, June 15 (1 pm ET)



Register for the webinar – Tuesday, June 20 (1 pm ET)



Does your agency offer differential pay based on an officer's educational attainment (Associate's, Bachelor's, or advanced degree)?

Click here to take our poll.



Dash cam video: Mich. troopers pull over boy, 10, accused of stealing SUV

When the SUV wouldn't pull over, OnStar was able to disable it. Once it stopped, the boy ran away but was quickly taken into custody



Bill named after slain Texas deputy becomes law, increasing penalties for catalytic converter thefts

The bill was named in honor of Deputy Darren Almendarez who was killed while trying to stop three men attempting to steal his vehicle's catalytic converter



State your case: Should an active shooter's manifesto be made public?

By Jim Dudley and Chief Joel Shults, EdD

There are many layers of complexity inherent in balancing transparency, public safety, and respect for the victims and their families

On-demand webinar: Using human performance science to inform police training and improve officer decision-making

By Police1 Staff

A deeper dive into how police trainers can integrate human factor science into police training

Get closer to Vision Zero.

Schedule a free demo to find out how a total community solution providing speed enforcement, ALPR and video can help change driver behavior and keep communities safer.

Take action today

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 © 2023 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: P1 Product Video Bulletin
To: McCarthy, Steven (POL)
Subject: Check out the latest Police1 Product Videos
Date: Thursday, January 26, 2023 5:16:47 PM

January 26, 2023 | View as webpage

Well-Equipped Lenco BearCat G3 for $286,153!

Lenco BearCats for any mission & budget. Prices range $242,558-$341,288.

Watch the full video here

BRINC Ball – Next Gen Throw Phone

New, ruggedized two-way communication device built to enhance de-escalation capabilities of law enforcement. 60+ ft audibility. 20+ hour talk time. Simply call to connect.

Watch Now

Recoil Kits Made in America

VirTra's durable hardware is manufactured in our own machine shop with high-quality materials.

See How We Do It

Artificial Intelligence is the future of law enforcement.

Law Enforcement Media Analysis, powered by IDOL, will save you time and resources with our Facial Recognition, ALPR and Object Detection built into one software solution for your video and picture forensic needs, and is currently free for a 30-day trial!

Streamlight's New Ultra-Bright Tactical USB-C Rechargeable Flashlight

The new ProTac® 2.0 produces 2,000 lumens without sacrificing run time.

Request a demo

Learn More about ProTac® 2.0

BMW R 1250 RT-P Lays Down Fastest Time

BMW Brand Ambassador Quinn Redeker ran the fastest time of all entrants during the 2022 Mid Atlantic Police Motorcycle Rodeo in Tysons Corner Virginia. Quinn is a retired police officer from the City of Ventura, CA and was riding a 2022 BMW R 1250 RT-P representing BMW Motorrad.

Click to watch the video

Connecting teams for disaster response

With FirstNet, first responders get the priority and preemption they need on a reliable, highly secure network – no matter the call.

Learn more at firstnet.com

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 © 2023 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Chicago mayor doesn"t want ShotSpotter; Video: Bees swarm LAPD volunteer
Date: Tuesday, May 16, 2023 5:20:59 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.

May 16, 2023 | View as webpage | Too many emails? Update Subscription Preferences

Trooper remains hospitalized, cop released after N.M. shooting

The police chief said he was “unbelievably proud” of officers’ response given the threat of the suspect, who was moving around, and the chaotic scene

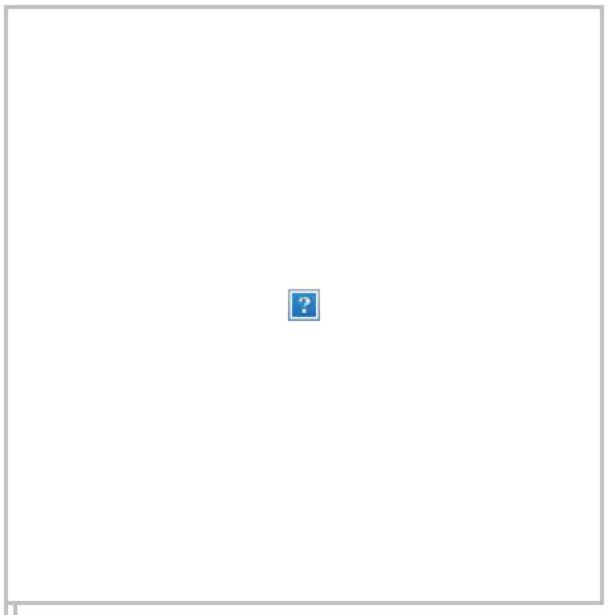
Chicago mayor promises new approach to CPD, including adding police detectives

Man sentenced to up to 92 years in prison for shooting Iowa deputy during robbery

Video: Bee swarm sends LAPD volunteer officer to hospital

Gov. rejects push for all N.J. police, firefighters to retire with pensions after 20 years

Colo. man tries to trade places with dog to avoid DUI arrest



Get closer to Vision Zero.



Schedule a free demo to find out how a total community solution providing speed enforcement, ALPR and video can help change driver behavior and keep communities safer.

Take action today

#TRAININGTUESDAY

Why focused training on one-handed shooting drills is crucial to officer survival

By Todd Fletcher

Don't make a bad day worse by failing to practice the shooting skills that could help you prevail

Seconds save lives: A review of Ed Monk's active shooter instructor class

By Warren Wilson

This school was very unique in that I felt I could walk out of Last Resort Firearms Training headquarters and teach a class with very little preparation

Webinar: Using human performance science to inform police training and improve officer decision-making

By Police1 Staff

A deeper dive into how police trainers can integrate human factor science into police training

Quiqlite TAQ Wallet - Stealth * Versatile * Super-Charged

THE WORLD'S ONLY tactical wallet with USB rechargeable LED flashlight, bottle opener, screwdriver, glass breaking tip and Carabiner.

Order Now

ON-DEMAND WEBINAR

Promotional interview tactics for success

Unique approaches to be more competitive in your promotional testing efforts

NATIONAL POLICE WEEK

Preparing your family for a critical incident: A checklist for first responders and their families

By Jaime Brower, Psy.D.

Proactive measures to navigate and support each other through challenging times

Fallen LEOs honored at National Peace Officers' Memorial Service

By Sarah Roebuck

During the service, a few stories of some of the fallen officers were highlighted

Photos, videos: Fallen LEOs mourned, remembered during Police Week

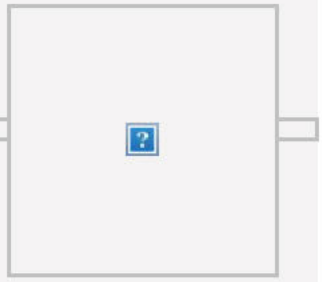
By Police1 Staff

A full calendar of events were held from May 10-16; here are scenes from this year's commemorative events

Sponsored Content

How this PD saves time and money with AWS Public Sector Partner SOMA Global

The SOMA platform has exceeded expectations, making sure critical emergency call-taking and dispatching continues.



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 © 2023 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Cop thrown into sinkhole by semi; LEOs save toddler from near-drowning
Date: Wednesday, June 28, 2023 12:46:56 PM

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

June 28, 2023 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

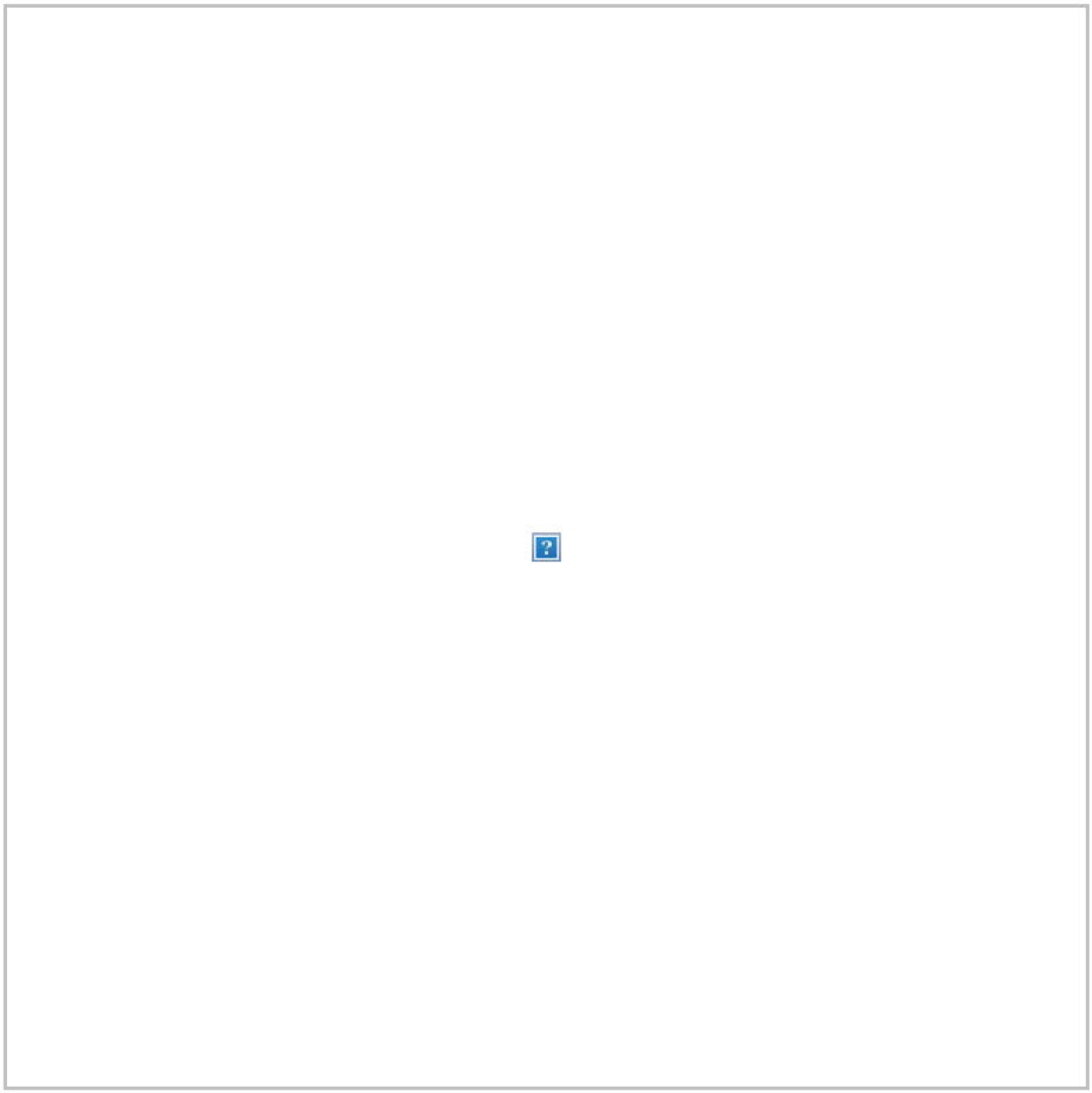
- Each speaker provided their own perspective which collectively led to an informative presentation.
- The panelists were very professional and had some great insights into the threat assessment process.
- The panel of speakers were very knowledgeable and had lots of good info.

These are just some of the responses from attendees of our recent webinar, "Building Safer Schools: How Law Enforcement and Educators Can Develop Effective Threat Assessment Teams to Stop School Violence" sponsored by L3Harris.

Click here to watch this online discussion to assess valuable insights into developing a comprehensive approach to threat assessment and school safety.

Stay safe,

— *The Police1 Team*



Officer pushed into sinkhole after tractor-trailer slams through barricade

The tractor-trailer was driving too fast for conditions and struck the officer's patrol vehicle, pushing the officer into the hole

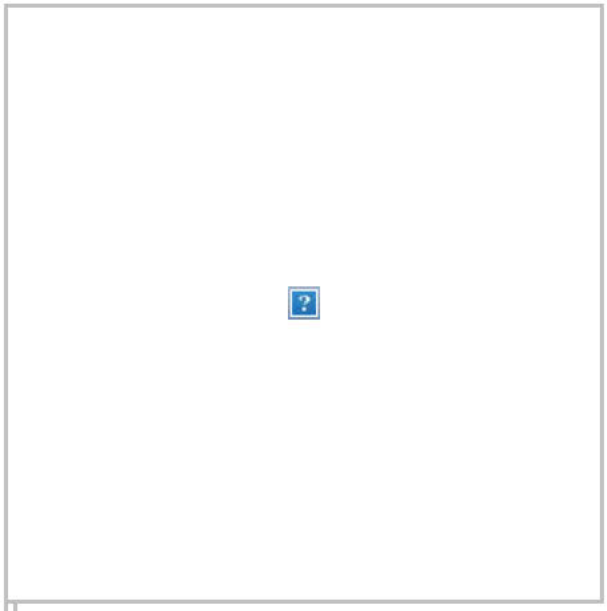
Watch: BWC video shows Mich. officers rescue toddler from attempted drowning by mother

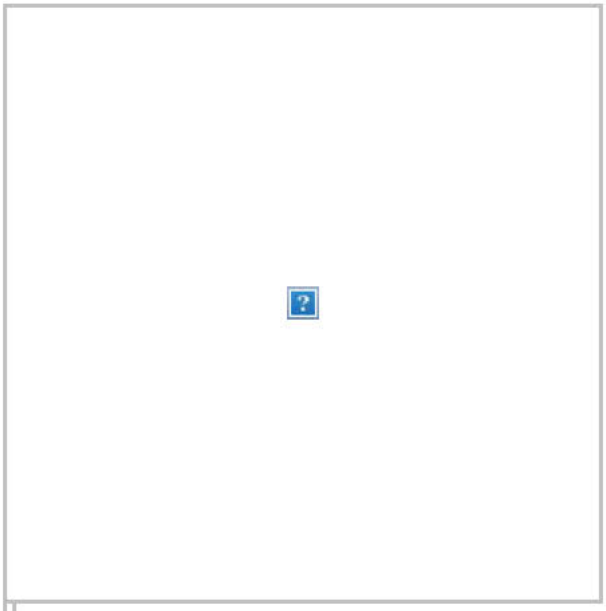
Pa. trooper killed in ambush lauded as a hero during funeral

Calif. police seize 5K pounds of illegal fireworks being manufactured at house

Watch: Teen in stolen vehicle shoots at deputy during pursuit

Ill. cop: 'My life changed forever' after being shot by suspect





ACTIVE SHOOTER PREVENTION

How an open mind can help officers prepare for, prevent and problem solve the active killers problem

By Lt. Dan Marcou

If you are honest enough to admit you do not possess an open mind, then aggressively strive to

develop one

How can we stop school shootings in America?

By Bradley D. Beach

Strategies should include reporting the signs, anonymous tip lines and behavioral threat assessments

How one agency eased the burden of vehicle crash reporting



Longmont PD adopted these tech tools to create new efficiencies and clear crashes faster.

Read more

5 reasons LE agencies should consider the Safe Fleet FOCUS H2 with ALPR



Powered by AI, this system is a valuable investment for police departments.

Learn more

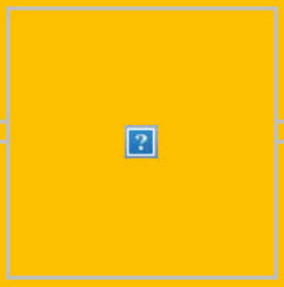


PHOTO OF THE WEEK

Knot just a school resource officer

School resource officer Nicholas Calello helps one of his students fix his tie before graduation

ROADWAY SAFETY

Protecting the pedestrian officer

By Sergeant (Ret.) Robert Bemis

LEOs rank among the highest number of "struck-by" fatalities of any responders. Could helmets be one answer to this safety crisis?

Research review: Preventing crashes and injuries among officers

By Hope M. Tiesman, PhD, and Sgt. Lou Maldonado (Ret.)

The first known scientific evaluation of an LE crash prevention program demonstrates significantly lower crash and injury rates - especially among patrol officers

Sponsored Content

Do’s and Don’ts of Social Media for Officers

Learn strategies for officers to enhance personal safety and security while using social media and guidance for officers with an active social media presence. Download Now





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 © 2023 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Cops save burglar shot by homeowner; LEO details burning car rescue
Date: Wednesday, February 1, 2023 1:34:44 PM

February 1, 2023 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Law enforcement officers are routinely exposed to highly stressful and potentially traumatizing events that can have lasting effects on their mental health. Unfortunately, the stigma of seeking mental health treatment among police and public safety personnel remains strong. Moreover, the prospect of talking to a therapist often conjures up fears of being evaluated by someone who doesn't understand the job.

Some agencies are fighting this stigma with a new program: mandatory annual mental wellness visits. Lexipol's upcoming webinar will explain what mental wellness visits are, how they can help reduce the stigma around mental health and how law enforcement agencies can develop a program.

Click here to reserve your seat.

Stay safe,

— *The Police1 Team*

TOP STORIES

Despite 'Cop City' protests, Atlanta moves forward with plan to build police training site

The city has pledged to enact certain environmental protections after consulting with a "community advisory committee"

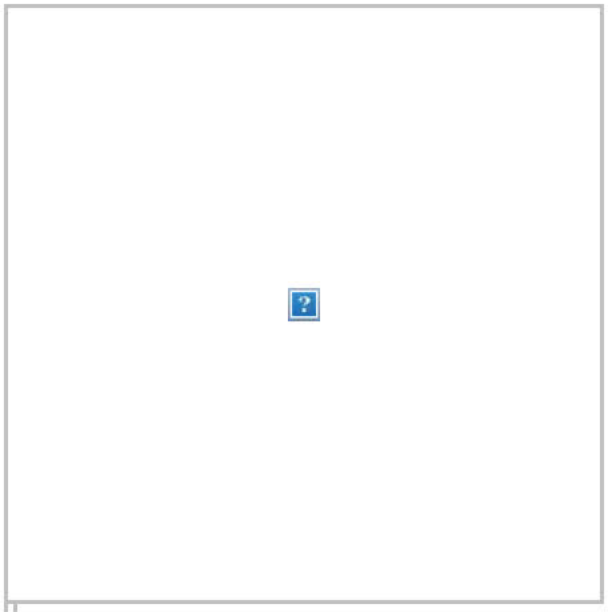
Calif. officer shot, killed by felon on probation; suspect arrested

Appeals court upholds restraining order on Ill. firearms ban

Judge to determine fate of last ex-Minneapolis cop charged in Floyd's death

Watch: Las Vegas officer details moments leading up to burning car rescue

'Not gonna let you die': Fla. officers save burglary suspect shot by homeowner



Why using the cloud is about more than just efficient storage



Police departments that store and manage data in the cloud can easily share it with other agencies, boosting collaborative efforts and closing more cases.

Learn More

FEATURED CONTENT



Having the last word

By Chief Joel F. Shults, Ed.D.

What should law enforcement leaders make of a retiring officer's last radio call that went viral for all the wrong reasons?



Bill Powers on homicide investigations: 'It is not about you, it is about a victim and the victim's family'

By Policing Matters Podcast

A veteran homicide detective discusses his book about a multidisciplinary investigation that started at an arson scene and ended nearly a year later with the case solved, plus he shares some pearls of wisdom for new detectives

DUTY TO INTERVENE: CASE STUDIES

Strengthening a culture of bystandership in Colorado



By Elisa DiTrolio
Unifying what loyalty means in policing today and understanding how police officers experience the same inhibitors to intervening as everyone else



Building an early intervention system: Lessons learned from the Yonkers Police Department

By Lieutenant Jared Singer
Early intervention systems take time and work to develop and implement and there is no "one size fits all" solution



SPONSORED CONTENT



How an ALPR system operating on in-car video system IDs vehicles & people-of-interest (white paper)

Improve situational awareness without separate hardware or increased officer distraction. Learn More.



FEATURED JOB



Find out more about BPD

Speak a second language? Receive a $2,000 bonus. The Bellingham Police Department is offering a $2,000 hiring bonus for those that speak a qualified second language. This bonus ends in June 2023. Don't miss this opportunity, apply today!

FEATURED RESOURCES



How to Buy Duty Gear (eBook)

Download this Police1 duty gear 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 © 2023 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Genetec newsletter
To: zzCrouse, David (POL)
Subject: David, see why IIoT matters
Date: Thursday, July 27, 2023 1:02:46 PM

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

Connecting the dots from Genetec

Hi David,

Everything you ever wanted to know about the Industrial Internet of Things (IIoT) is here! We even included real-life customer examples to give you ideas about how your team can connect IIoT sensors to get more from your physical security system.

Happy reading,

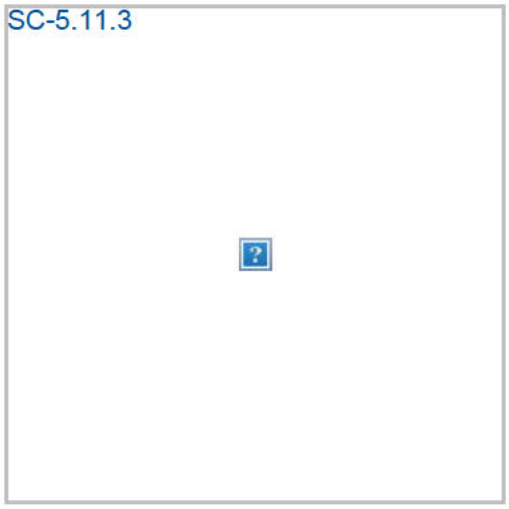
Julie Cadieux, **Senior Editor**
jcadieux@genetec.com

Product updates

Security Center 5.11.3

The latest release simplifies password management, allows you to schedule automatic firmware updates, and create dashboard customizations.

Read →





Take SIP calls on the go

The new version of Sipelia™ turns your mobile phone or tablet into a powerful security communication device.

← Read

Want better ALPR capture rates?

AutoVu™ Sharp Z3, our ALPR solution, has major new features

like stereoscopy, analytics, and dual exposure.

Read →

ALPR-AutoVu

Industrial Internet of Things

IoT-IIoT

Why IIoT matters

Find out how cloud, cybersecurity, unification, and AI impact the success of your IIoT journey.

← Read

Tips & tricks

TechDoc Hub

Check out the Genetec™ Mobile Getting Started Guide to learn how to perform Security Desk monitoring functions from your smartphone.

Read →

Genetec-mobile

people-detection

How does YOLO work?

Learn about object detection in video analytics, and why everyone's talking about the YOLO algorithm.

← Read

ClearID

Looking for ways to ensure security compliance and audit readiness?

Discover a simplified auditing process that allows you to schedule or manually launch access reviews through a self-service portal.

Simplify the audit process with ClearID

Get the updates you need

Select products of interest, preferred language, and more in our email preference center.

Manage your preferences →

View this online · Manage your preferences · Unsubscribe

Genetec Inc.
2280 Alfred-Nobel Blvd., Montreal, QC H4S 2A4 Canada

© 2023 Genetec Inc. TM trademark of Genetec Inc.

From: Genetec newsletter
To: Connor, Debora (POL)
Subject: Debora, see why IIoT matters
Date: Thursday, July 27, 2023 1:01:42 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.

Connecting the dots from Genetec

Hi Debora,

Everything you ever wanted to know about the Industrial Internet of Things (IIoT) is here! We even included real-life customer examples to give you ideas about how your team can connect IIoT sensors to get more from your physical security system.

Happy reading,

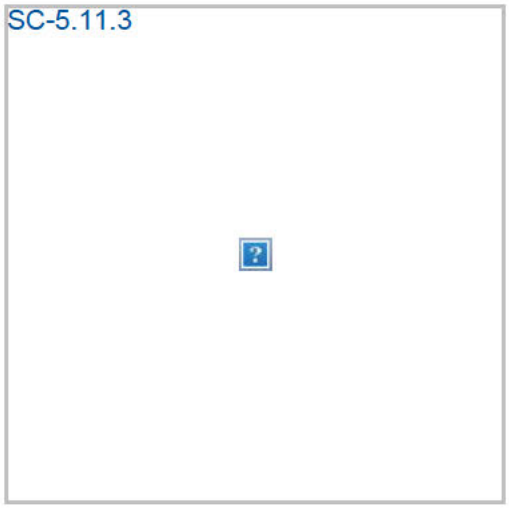
Julie Cadieux, **Senior Editor**
jcadieux@genetec.com

Product updates

Security Center 5.11.3

The latest release simplifies password management, allows you to schedule automatic firmware updates, and create dashboard customizations.

Read →





Take SIP calls on the go

The new version of Sipelia™ turns your mobile phone or tablet into a powerful security communication device.

← Read

Want better ALPR capture rates?

AutoVu™ Sharp Z3, our ALPR solution, has major new features

like stereoscopy, analytics, and dual exposure.

Read →

ALPR-AutoVu

Industrial Internet of Things

IoT-IIoT

Why IIoT matters

Find out how cloud, cybersecurity, unification, and AI impact the success of your IIoT journey.

← Read

Tips & tricks

TechDoc Hub

Check out the Genetec™ Mobile Getting Started Guide to learn how to perform Security Desk monitoring functions from your smartphone.

Read →

Genetec-mobile

people-detection

How does YOLO work?

Learn about object detection in video analytics, and why everyone's talking about the YOLO algorithm.

← Read

ClearID

Looking for ways to ensure security compliance and audit readiness?

Discover a simplified auditing process that allows you to schedule or manually launch access reviews through a self-service portal.

Simplify the audit process with ClearID

Get the updates you need

Select products of interest, preferred language, and more in our email preference center.

Manage your preferences →

View this online · Manage your preferences · Unsubscribe

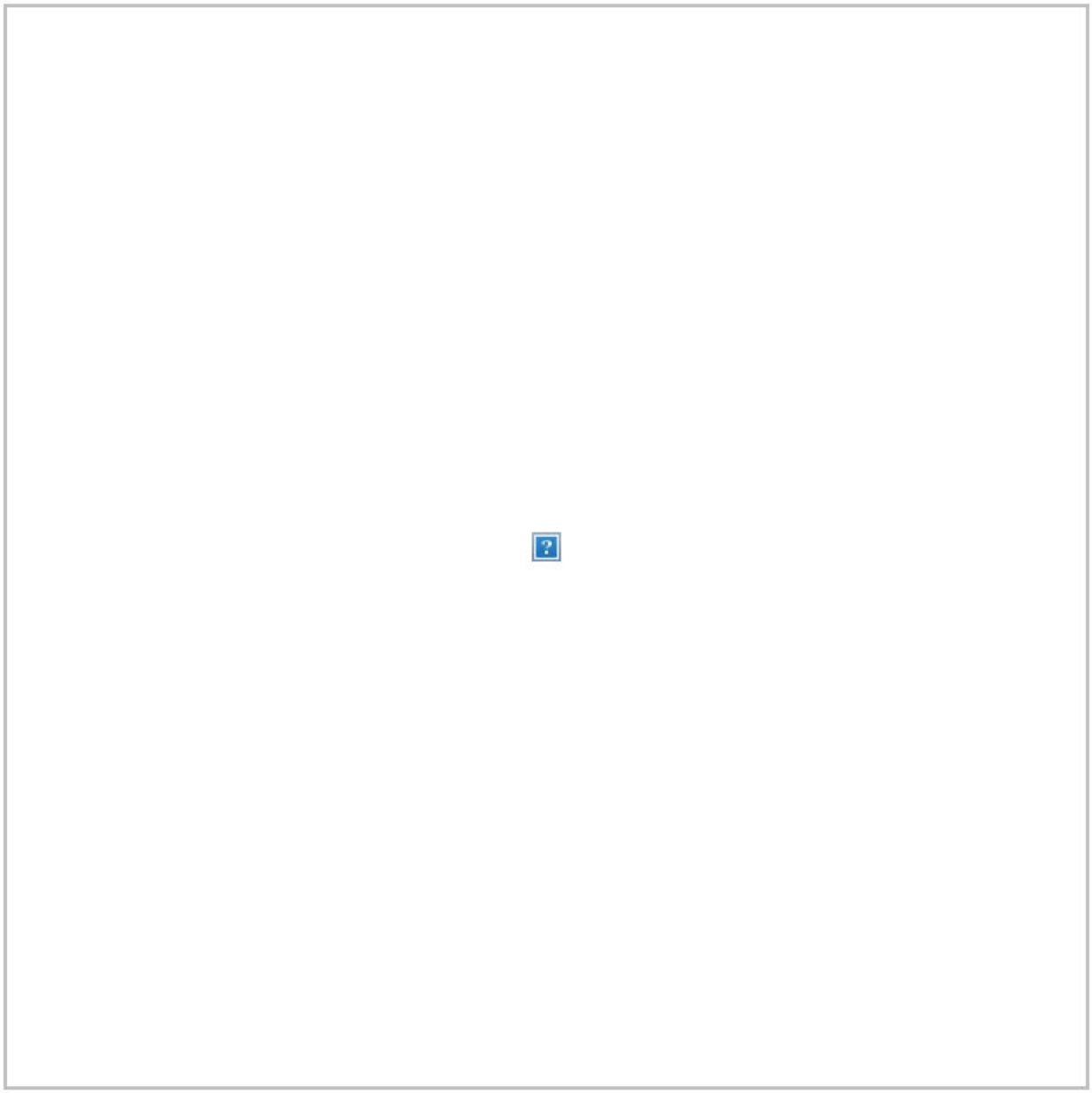
Genetec Inc.
2280 Alfred-Nobel Blvd., Montreal, QC H4S 2A4 Canada

© 2023 Genetec Inc. TM trademark of Genetec Inc.

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Deputy fatally shot, gunman steals patrol car; LE applicant age raised
Date: Wednesday, July 5, 2023 1:15:36 PM

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

July 5, 2023 | View as webpage | Too many emails? Update Subscription Preferences



Suspect fatally shoots Ga. deputy, flees in his patrol car

The deputy was conducting a traffic stop when he determined the car was stolen and the suspect was wanted for several burglaries

N.Y. State Police raise maximum age for trooper candidates

Officer fatally shot by domestic violence suspect in hospital

Bystander radios for help after trooper collapses from heat exhaustion

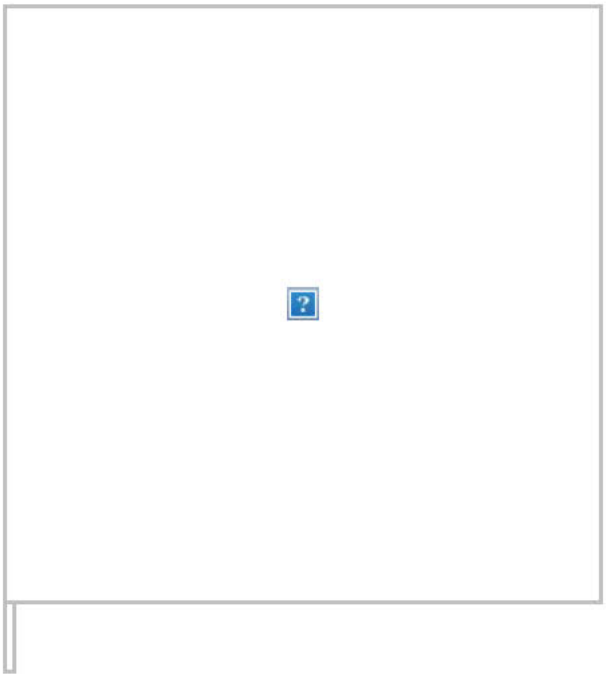
Mass. officers rescue woman trapped in mud for at least 3 days after hikers hear screams

Get a Free Patch From Hero's Pride



Hero's Pride is giving away their limited-edition free patch to the first 100 law enforcement officers who request one!

Get Your Free Patch Now!



FEATURED CONTENT

The Texas outlet mall active shooter: The tragedy and the triumph

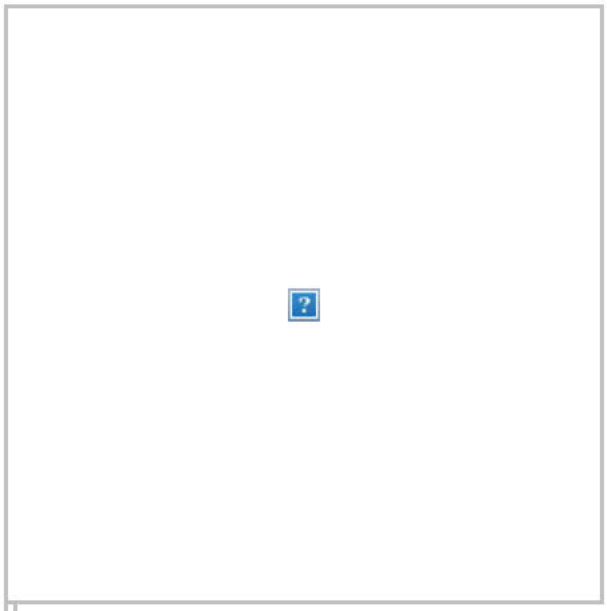
By Lt. Dan Marcou

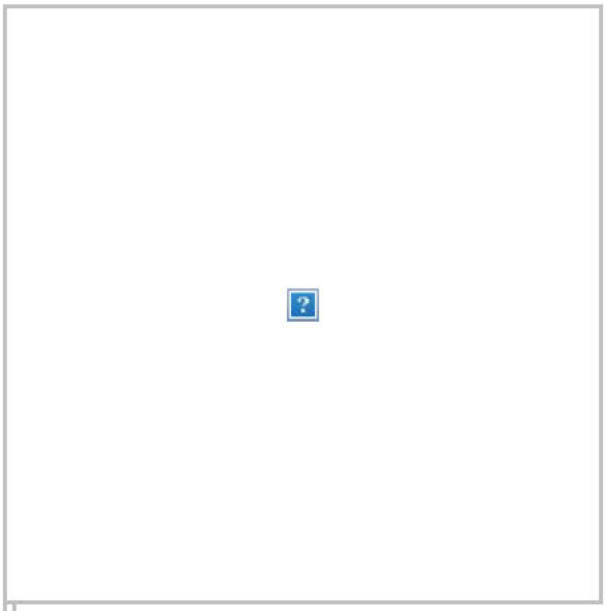
To the officer who stopped the killing, we thank you for inspiring the entire law enforcement profession with your determined, courageous and effective response

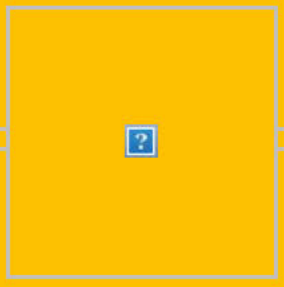
Creating a nexus between workload and costs: A case study from Ocean View PD

By Jon M. Shane, Ph.D.

By analyzing the type and frequency of calls for service, chiefs can ensure they are using resources effectively and efficiently while maintaining officer well-being







POLICING MATTERS PODCAST

How a threat assessment team tracks students of concern

"In reality, in the 2020s, if we are not looking at the digital footprint of a student of concern, we are really not doing a comprehensive threat assessment."

COMMUNITY POLICING

D.C.'s Special Liaison Branch builds positive police-public relations

By James Careless

"The SLB is all about having officers who understand and mirror the communities that they serve."

A small agency with big ideas

By Chief Joel F. Shults, Ed.D.

The Willard Police Department offers a template for community outreach and engagement

How winning an art contest connected me to the community I serve

By Elizabeth Prillinger

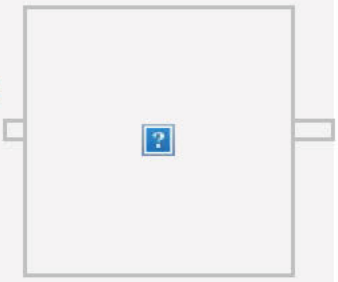
Police leaders would be wise to cultivate the intrinsic skills and talents of their officers in purposeful

ways to fortify meaningful connections with communities

Sponsored Content

5 reasons LE agencies should consider the Safe Fleet FOCUS H2 with ALPR

Powered by AI, this system is a valuable investment for police departments.



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 © 2023 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Pack, Noah (POL)
To: Cyr, Mark (POL)
Subject: DRAFT/NOTES
Date: Thursday, October 12, 2023 4:55:22 PM

Hi John,

There were a number of changes to the policy in this update, and the organization of the document was changed to the point where a version to version comparison is not particularly illuminating. To help with this, here are some of the highlights:

Authorized/Prohibited Uses

- Revised authorized uses to emphasize the Department's prioritization of ALPR use for serious public safety and homeland security matters
- Added authorized use for motor vehicle pursuit follow-up, due to frequent pursuit termination for public safety and de-escalation
- Added explicit restriction against use for immigration enforcement

Legal Considerations

- Added section on legal considerations to address McCarthy case law

Search Procedures

- Revised section to provide clear guidelines on search justification & documentation
- Added requirement to limit searches to be reasonable and consistent with the geographic and temporal needs of the incident or investigation
- Added clear authorization for Fusion Center staff to deny overly intrusive or improper requests

Manual Hotlist Entries

- Reduced maximum expiration time from 1 year to 30 days, with built-in automatic expiration to prevent user error or misuse
- Added requirement for supervisory approval, unless exigent circumstances
- Added notice to give special attention to rental and short-term use vehicles and incidents that may be quickly resolved

Use Non-Departmental ALPR Systems:

- Added requirement that limits access to any outside systems

- Added cautionary notice on different technology/retention of other systems

Other Miscellaneous Updates:

- Added requirement that user training must include discussion of privacy considerations and best practices
- Improved and clarified section on verifying LPR hits prior to taking enforcement action
- Added that retained LPR data does not include any video or audio recordings or intentional photos of persons
- Added notice/requirement of system time verification protocols to ensure that accurate data can be confirmed and inaccurate data can be identified

From: PoliceGrantsHelp Alert
To: Tulipano, Michael (POL)
Subject: Find Grant Money to Help Fund Your LPR Systems
Date: Tuesday, November 28, 2023 11:19:15 AM

View as webpage | Too many emails? Update Subscription Preferences

Find Grant Money to Pay for ELSAG Automatic License Plate Reader Technology



Find Grant Money to Pay for ELSAG Automatic License Plate Reader Technology



We have partnered with PoliceGrantsHelp.com to help you access government grant dollars

ELSAG Plate Hunter ALPR systems bring incredible efficiencies to real-time policing, security and investigations. Our solutions include fixed, mobile, solar-powered, video-camera and custom plate readers. Each is purpose-built to provide maximum performance for the lowest investment to effectively aid your law enforcement missions. These force-multiplying systems are ideal for:

- Recovering stolen vehicles and license plates
- Removing unregistered vehicles and unlicensed drivers from roads
- Finding missing persons
- Finding vehicles suspected of involvement in unlawful activity
- Parking management and enforcement
- Collecting criminal intelligence
- Permit validation and tolling
- Collection of traffic data

Button - Get Details
Button - Get Details
Button - Get Details
Button - Get Details
Footer - Email and website. leonardocompany-us.com/lmr

If you do not wish to receive future PoliceGrantsHelp Product Alerts, please unsubscribe.
To change your email address, update your profile. © : PoliceGrantsHelp.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: PoliceGrantsHelp Alert
To: Heath, Brendan (POL)
Subject: Find Grant Money to Help Fund Your LPR Systems
Date: Tuesday, November 28, 2023 11:19:39 AM

View as webpage | Too many emails? Update Subscription Preferences

Find Grant Money to Pay for ELSAG Automatic License Plate Reader Technology



Find Grant Money to Pay for ELSAG Automatic License Plate Reader Technology



We have partnered with PoliceGrantsHelp.com to help you access government grant dollars

ELSAG Plate Hunter ALPR systems bring incredible efficiencies to real-time policing, security and investigations. Our solutions include fixed, mobile, solar-powered, video-camera and custom plate readers. Each is purpose-built to provide maximum performance for the lowest investment to effectively aid your law enforcement missions. These force-multiplying systems are ideal for:

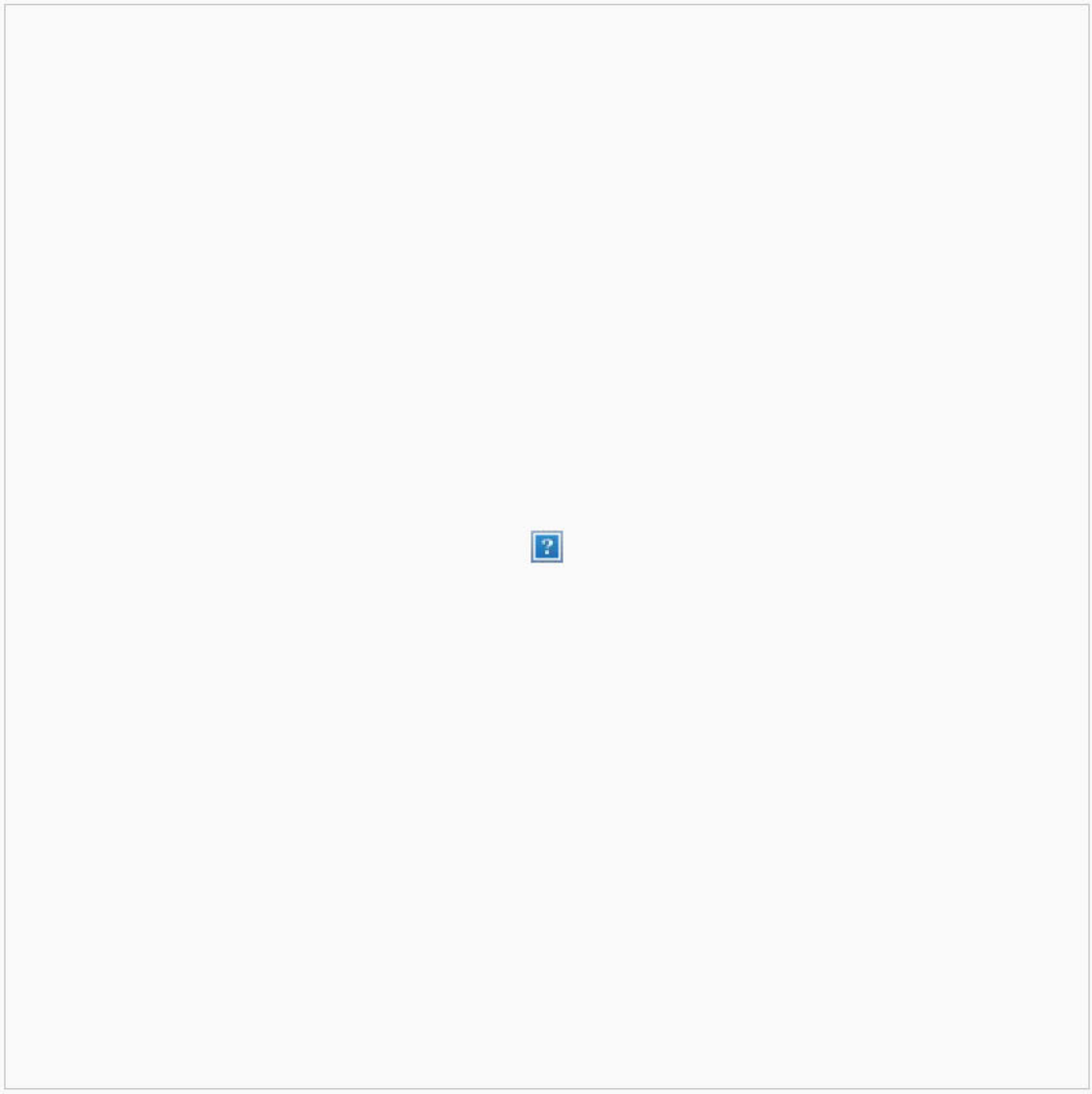
- Recovering stolen vehicles and license plates
- Removing unregistered vehicles and unlicensed drivers from roads
- Finding missing persons
- Finding vehicles suspected of involvement in unlawful activity
- Parking management and enforcement
- Collecting criminal intelligence
- Permit validation and tolling
- Collection of traffic data

Button - Get Details
Button - Get Details
Button - Get Details
Button - Get Details
Footer - Email and website. leonardocompany-us.com/lmr

If you do not wish to receive future PoliceGrantsHelp Product Alerts, please unsubscribe.
To change your email address, update your profile. © : PoliceGrantsHelp.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: PoliceGrantsHelp Alert
To: Heath, Brendan (POL)
Subject: Find Grant Money to Pay for ELSAG® Automatic License Plate Reader Technology
Date: Thursday, February 23, 2023 7:03:52 AM

View this email in your browser



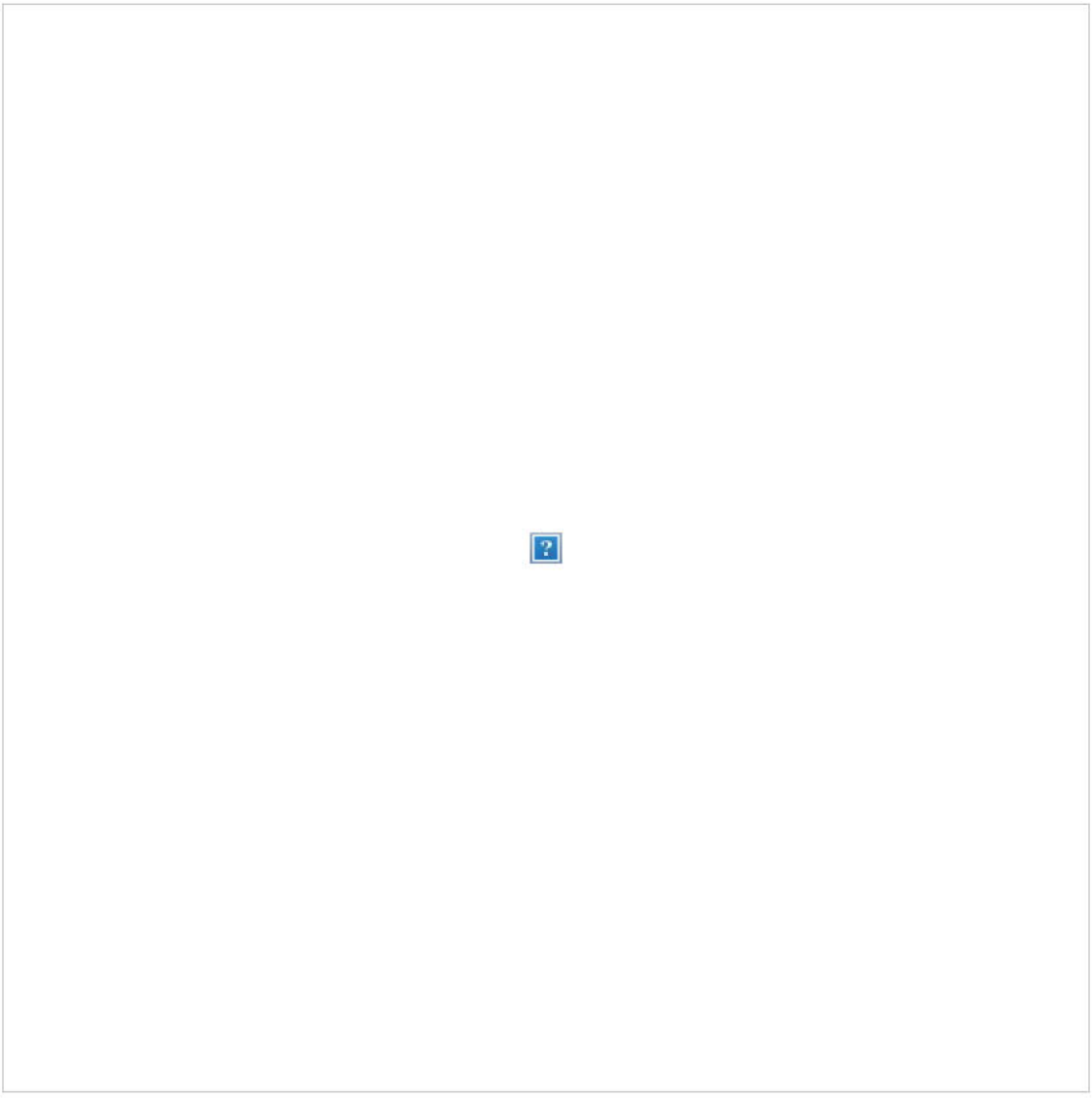
Find Grant Money to Pay for ELSAG® Automatic License Plate Reader Technology

We have partnered with PoliceGrantsHelp.com to help you access government grant dollars

ELSAG Plate Hunter ALPR systems bring incredible efficiencies to real-time policing, security and investigations. Our solutions include fixed, mobile, solar-

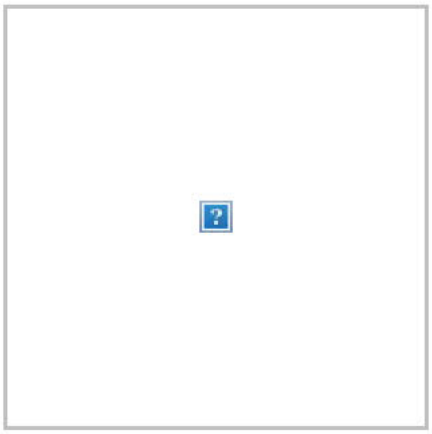
powered, video-camera and custom plate readers. Each is purpose-built to provide maximum performance for the lowest investment to effectively aid your law enforcement missions. These force-multiplying systems are ideal for:

- Recovering stolen vehicles and license plates
- Removing unregistered vehicles and unlicensed drivers from roads
- Finding missing persons
- Finding vehicles suspected of involvement in unlawful activity
- Parking management and enforcement
- Collecting criminal intelligence
- Permit validation and tolling
- Collection of traffic data



There’s no better time to deploy ELSAG automatic license plate readers.

Get FREE ALPR Grant Help



For information about ELSAG® Plate Hunter ALPR systems, visit
leonardocompany-us.com
Selex ES Inc., a Leonardo company 4221 Tudor Lane Greensboro NC USA 27410-8105

If you do not wish to receive future PoliceGrantsHelp Product Alerts, please unsubscribe .
To change your email address, update your profile . © : PoliceGrantsHelp.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: PoliceGrantsHelp Alert
To: Tulipano, Michael (POL)
Subject: Find Grant Money to Pay for ELSAG® Automatic License Plate Reader Technology
Date: Thursday, February 23, 2023 7:02:25 AM

View this email in your browser

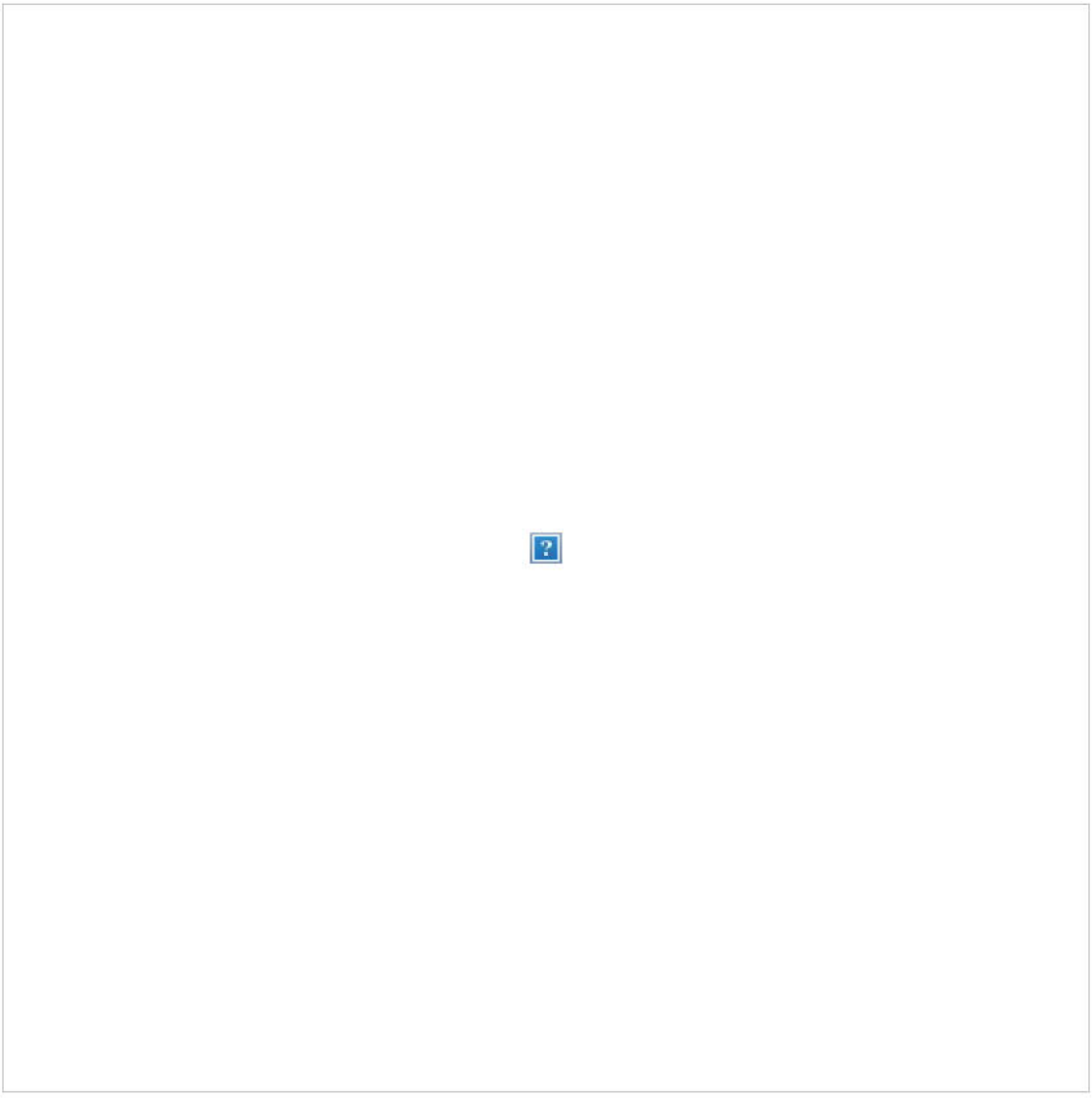
Find Grant Money to Pay for ELSAG® Automatic License Plate Reader Technology

We have partnered with PoliceGrantsHelp.com to help you access government grant dollars

ELSAG Plate Hunter ALPR systems bring incredible efficiencies to real-time policing, security and investigations. Our solutions include fixed, mobile, solar-

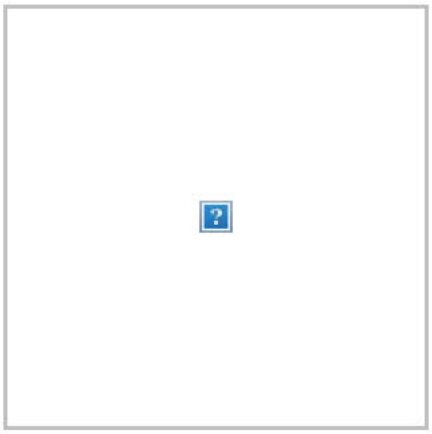
powered, video-camera and custom plate readers. Each is purpose-built to provide maximum performance for the lowest investment to effectively aid your law enforcement missions. These force-multiplying systems are ideal for:

- Recovering stolen vehicles and license plates
- Removing unregistered vehicles and unlicensed drivers from roads
- Finding missing persons
- Finding vehicles suspected of involvement in unlawful activity
- Parking management and enforcement
- Collecting criminal intelligence
- Permit validation and tolling
- Collection of traffic data



There’s no better time to deploy ELSAG automatic license plate readers.

Get FREE ALPR Grant Help



For information about ELSAG® Plate Hunter ALPR systems, visit
leonardocompany-us.com
Selex ES Inc., a Leonardo company 4221 Tudor Lane Greensboro NC USA 27410-8105

If you do not wish to receive future PoliceGrantsHelp Product Alerts, please unsubscribe .
To change your email address, update your profile . © : PoliceGrantsHelp.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: PoliceGrantsHelp Alert
To: Tulipano, Michael (POL)
Subject: Find Grant Money to Pay for ELSAG® Automatic License Plate Reader Technology
Date: Tuesday, June 6, 2023 8:45:03 AM

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

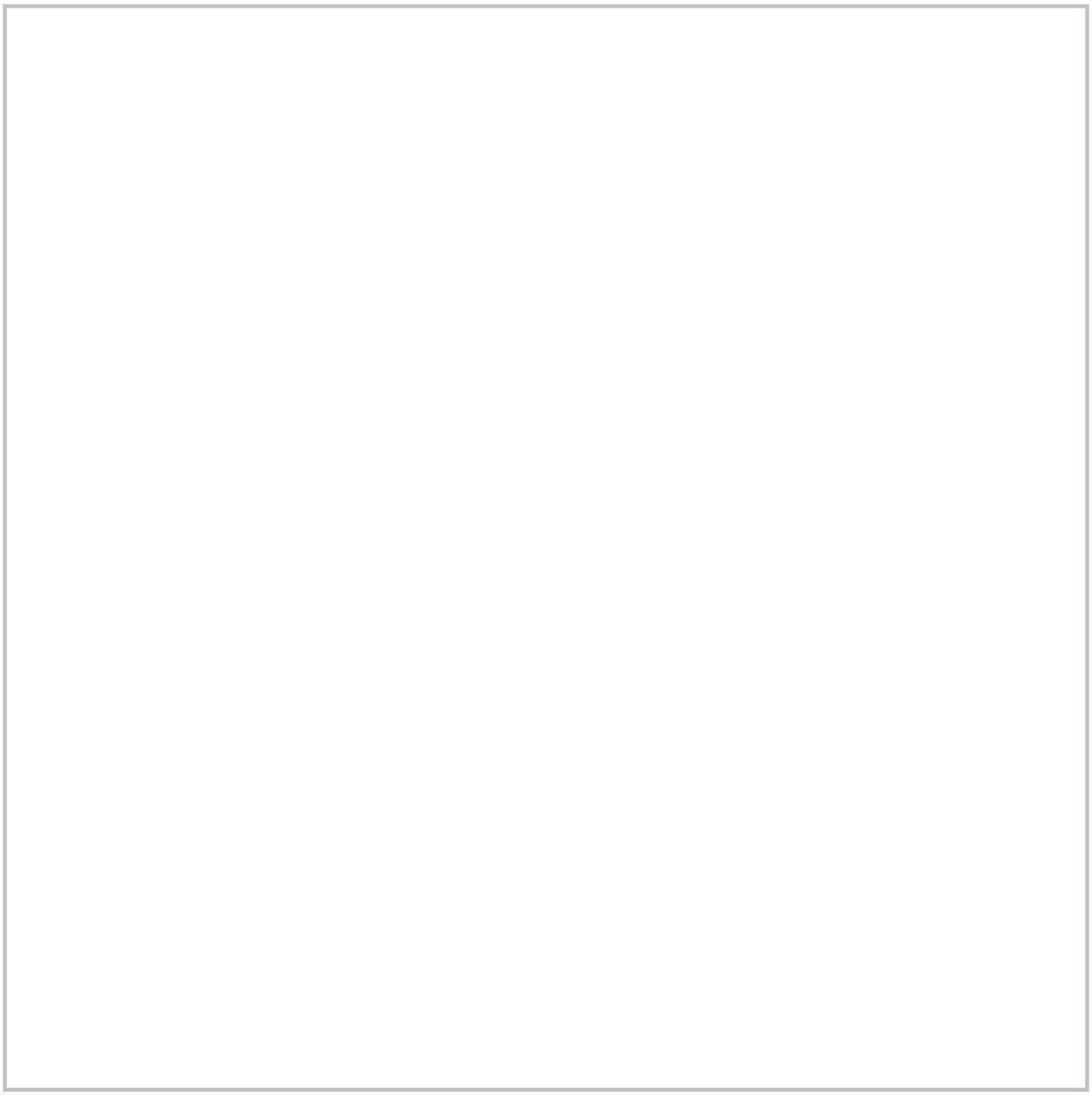
View this email in your browser

Find Grant Money to Pay for ELSAG® Automatic License Plate Reader Technology

We have partnered with PoliceGrantsHelp.com to help you access government grant dollars

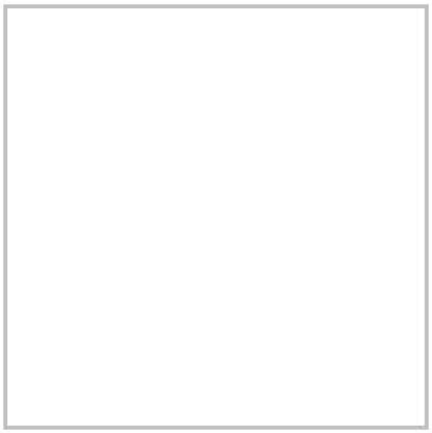
ELSAG Plate Hunter ALPR systems bring incredible efficiencies to real-time policing, security and investigations. Our solutions include fixed, mobile, solar-powered, video-camera and custom plate readers. Each is purpose-built to provide maximum performance for the lowest investment to effectively aid your law enforcement missions. These force-multiplying systems are ideal for:

- Recovering stolen vehicles and license plates
- Removing unregistered vehicles and unlicensed drivers from roads
- Finding missing persons
- Finding vehicles suspected of involvement in unlawful activity
- Parking management and enforcement
- Collecting criminal intelligence
- Permit validation and tolling
- Collection of traffic data



There’s no better time to deploy ELSAG automatic license plate readers.

Get FREE ALPR Grant Help



For information about ELSAG® Plate Hunter ALPR systems, visit

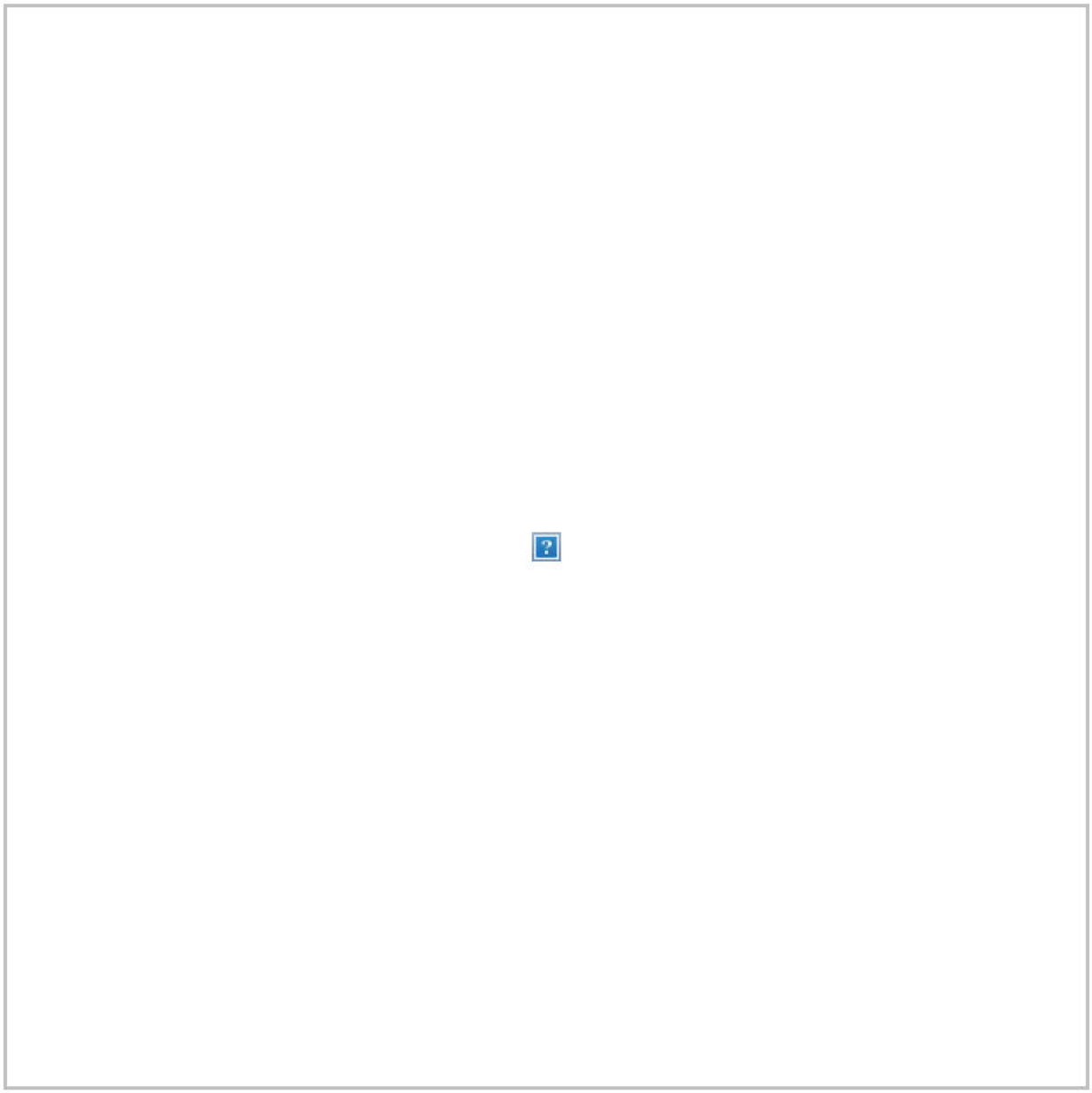
leonardocompany-us.com

Selex ES, LLC, a Leonardo company, 4221 Tudor Lane Greensboro NC USA 27410-8105

If you do not wish to receive future PoliceGrantsHelp Product Alerts, please unsubscribe .
To change your email address, update your profile . © : PoliceGrantsHelp.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Fla. schools want own police force; LAPD recruits may make $86K
Date: Wednesday, August 2, 2023 1:46:16 PM

August 2, 2023 | View as webpage | Too many emails? Update Subscription Preferences



Tentative contract: LAPD cops' starting pay may increase by 11%

The contract would boost annual starting pay for LAPD recruits from $74,000 to around $86,000

La. deputy marshal shot, killed while serving warrant

'Our dog saved the lives of the officers and citizens': Calif. K-9 killed in shooting

Reward increased for arrests of ‘anarchists’ who torched Atlanta police motorcycles

Fla. school district considers creating its own police force

City looking to reinstate its volunteer reserve police force

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

Keep our kids safe.



Jenoptik’s proven speed cameras, bus stop arm and civil security solutions modify driver behavior to increase school zone safety and deliver peace of mind for parents.

Learn more

CASE REVIEWS



Qualified immunity appropriate for shooting lasting 2 seconds

By Ken Wallentine

The court determines whether to grant officers qualified immunity for allegations of excessive force



The rise and fall of James 'Whitey' Bulger

By Mike Callahan

Recruiting and operating organized crime gang members and bosses as long-term confidential criminal informants is a dangerous game for law enforcement officers

Get a Free Patch From Hero's Pride



Hero's Pride is giving away their limited-edition free patch to the first 100 law enforcement officers who request one!

Get Your Free Patch Now!

Lexipol Annual Conference: Closing Keynote by Gordon Graham!



Chose from 10 sessions designed for professionals in law enforcement. Topics include recruitment, legislative trends, policy, tactics, training, wellness, accreditation and more!

Register Free Now

OFFICER SURVIVAL



Deputy Eddy Luna's fight for physical and emotional survival after the gun smoke cleared

By Lt. Dan Marcou

"Everything was in slow motion, and I saw a flash. Suddenly I was down on my stomach, but I didn't even know I was shot."



Developing a respect-based police survival attitude

By Lt. Dan Marcou

Respect may be the most important thing that contributes to an officer's safety – here's why

Sponsored Content

How an Ariz. PD is using software to connect domestic violence survivors with help

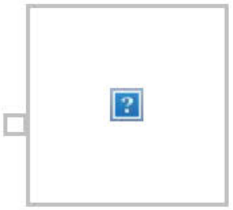
The El Mirage PD uses cloud-based case management software to provide information and support services to victims impacted by violence and trauma.



FEATURED JOB

MPD Entry-Level & Lateral Officer Positions Available

Apply Today!



Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

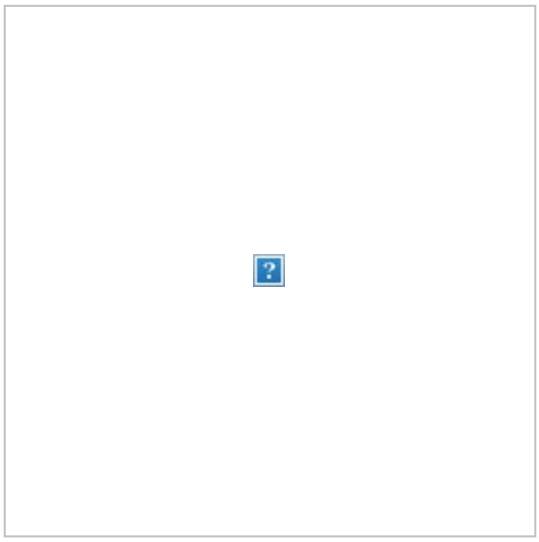
If you do not want to receive this newsletter, you can opt-out here.

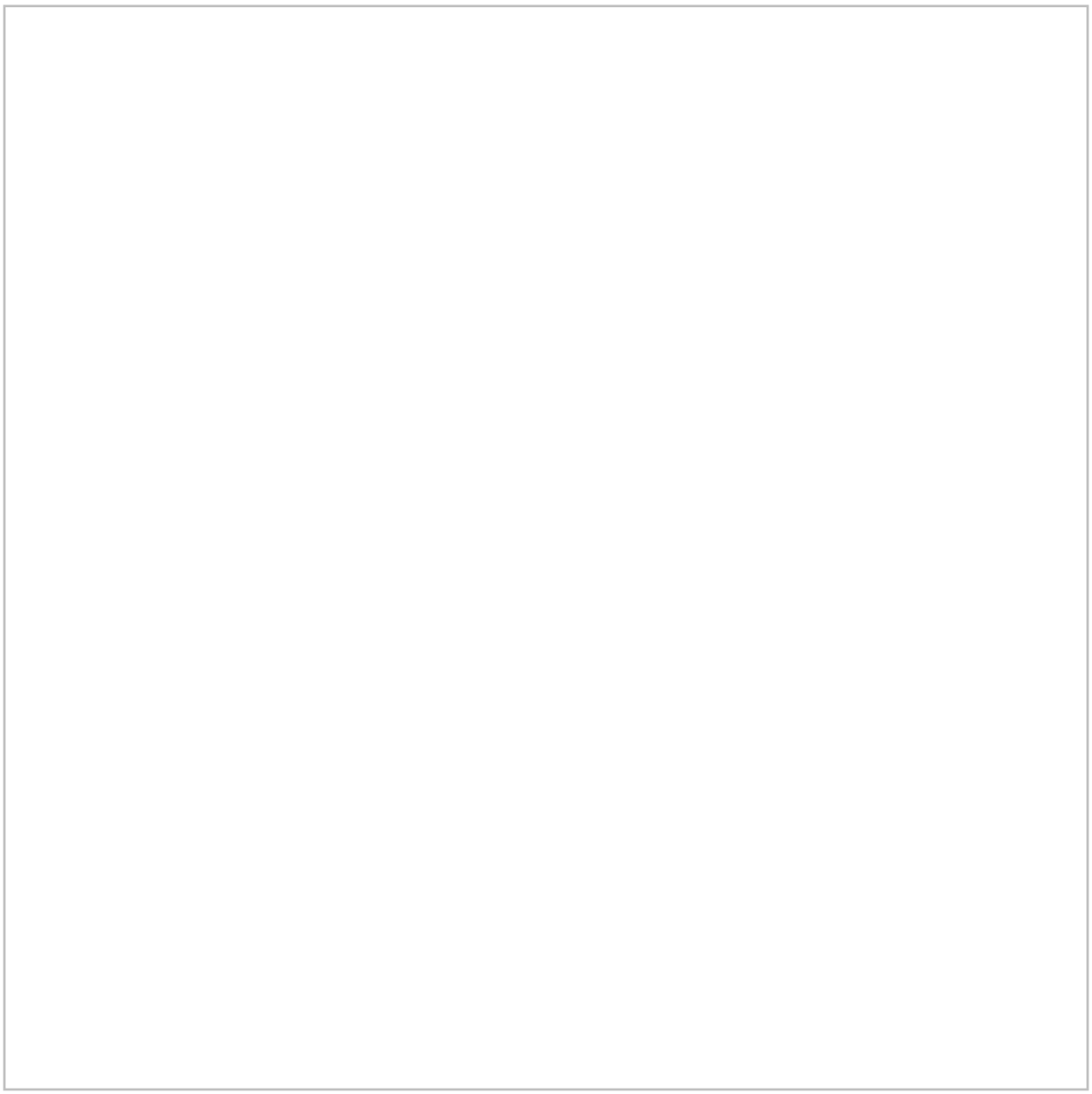
If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2023 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: International Homicide Investigators Association
To: McDermott, Karen (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 1:07:49 PM

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





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

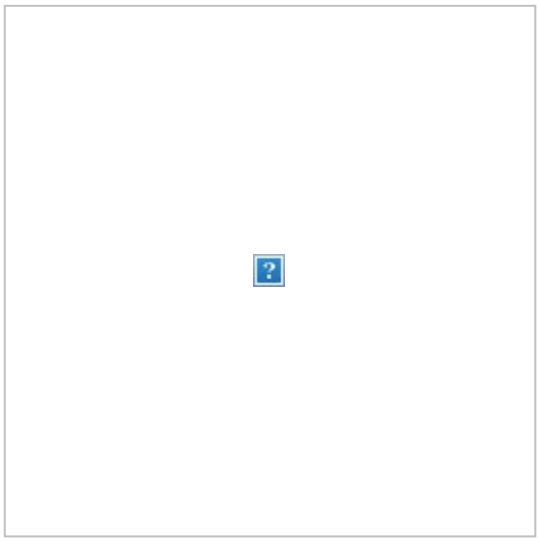
For more information on FINDER visit their website or contact them today!.

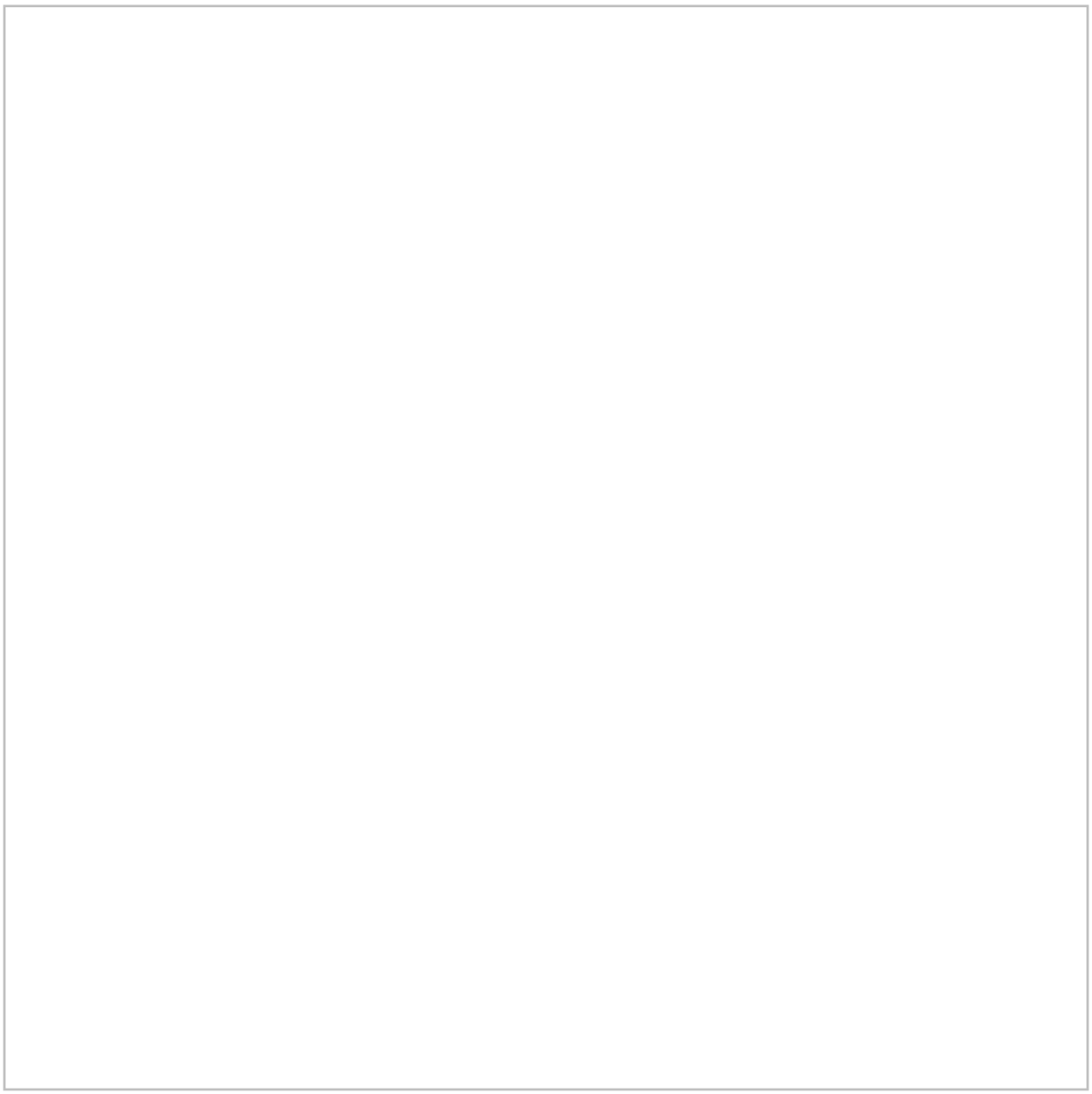
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Robertson, AnnMarie (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 1:07:48 PM

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





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

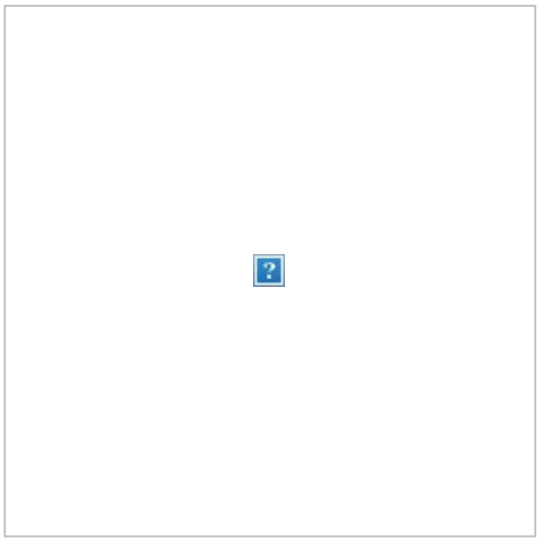
For more information on FINDER visit their website or contact them today!.

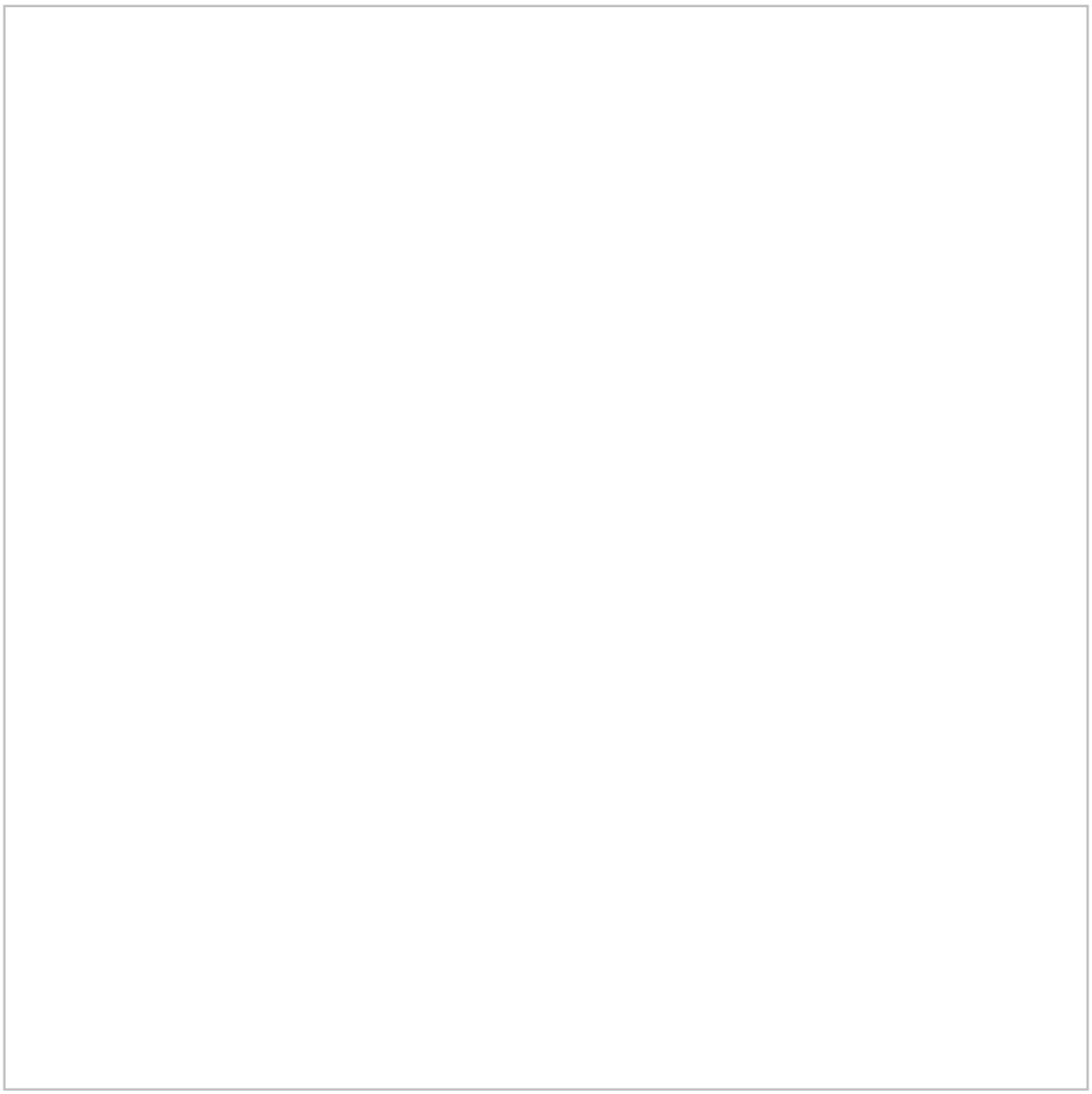
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Santa, Daniel (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:55:19 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.





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

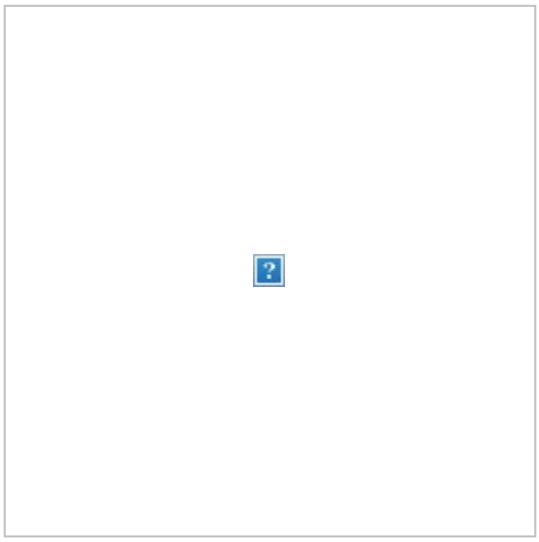
For more information on FINDER visit their website or contact them today!.

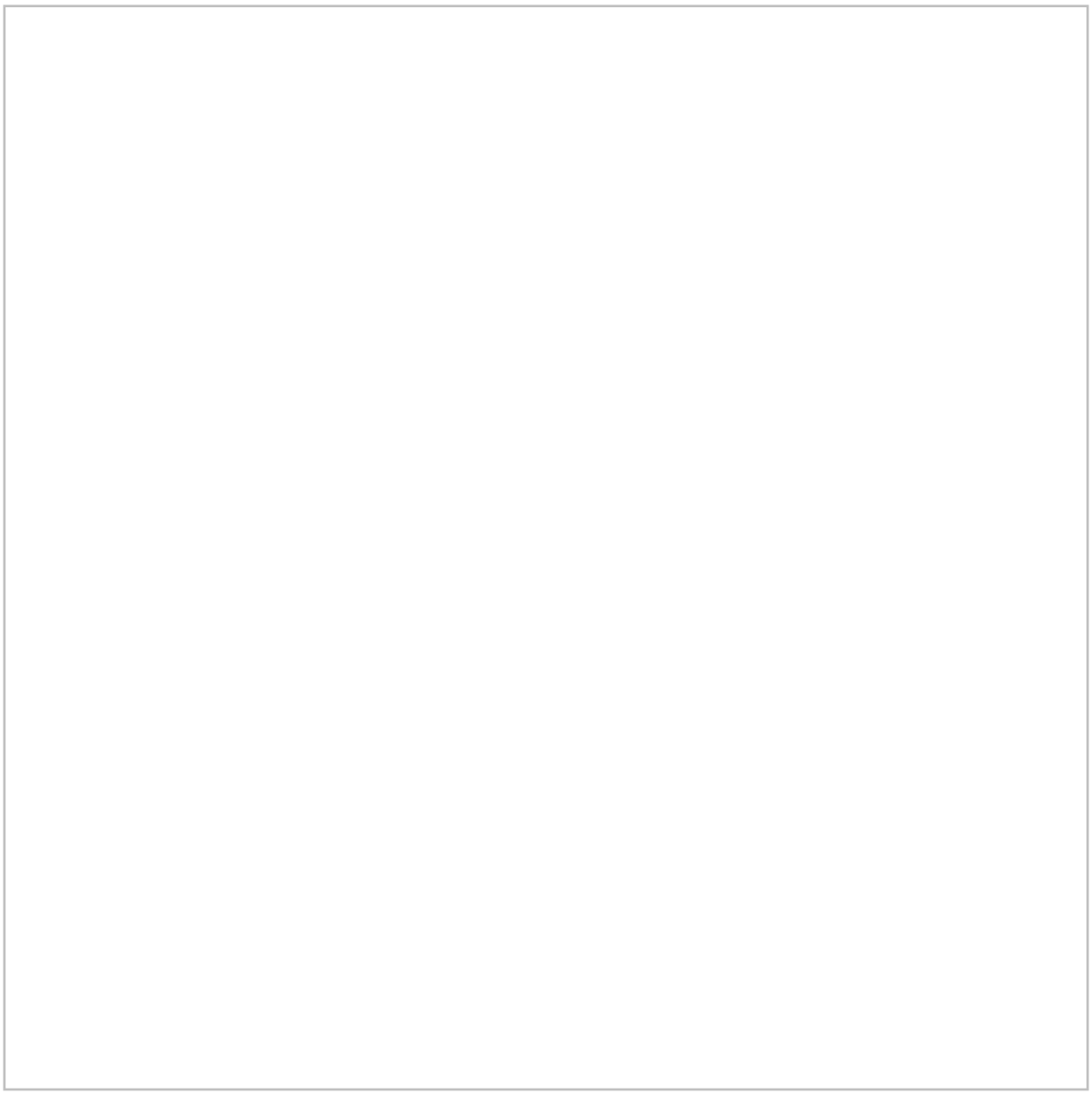
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Gregg, Theodore (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:55:18 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.





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

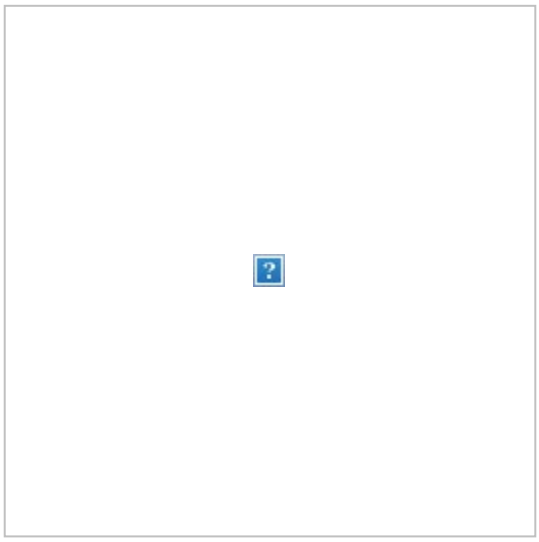
For more information on FINDER visit their website or contact them today!.

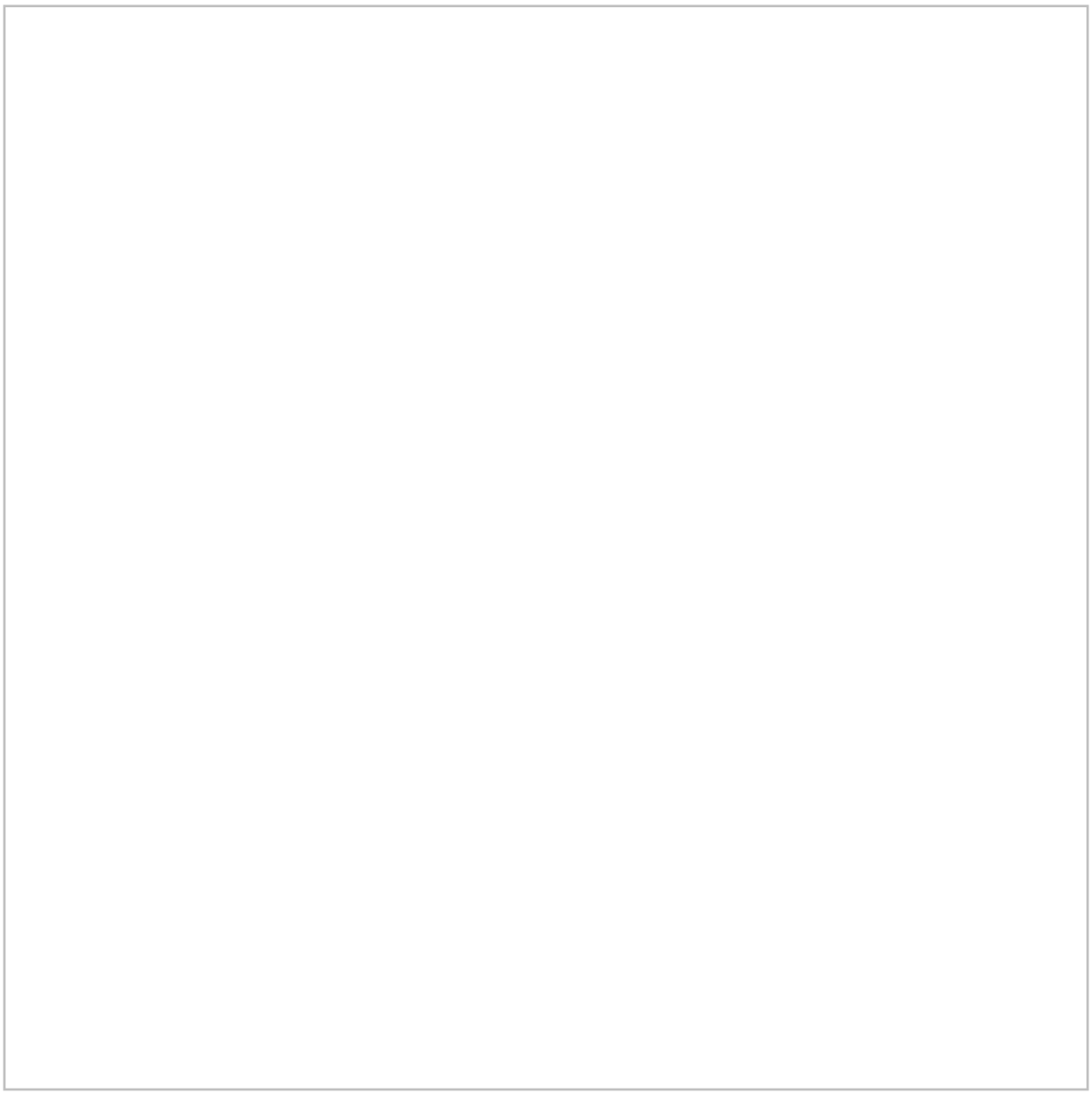
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Falzone, Jessica (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:55:18 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.





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

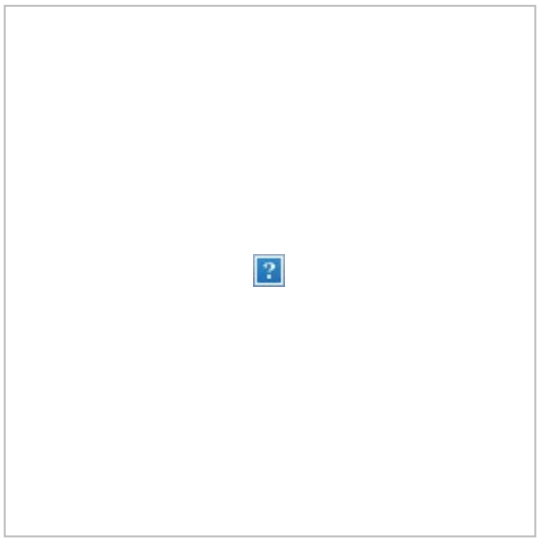
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Leblanc, Shawn (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:55:17 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.



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

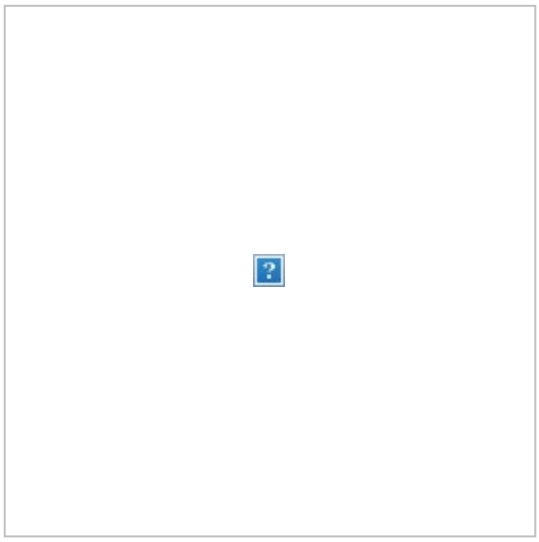
For more information on FINDER visit their website or contact them today!.

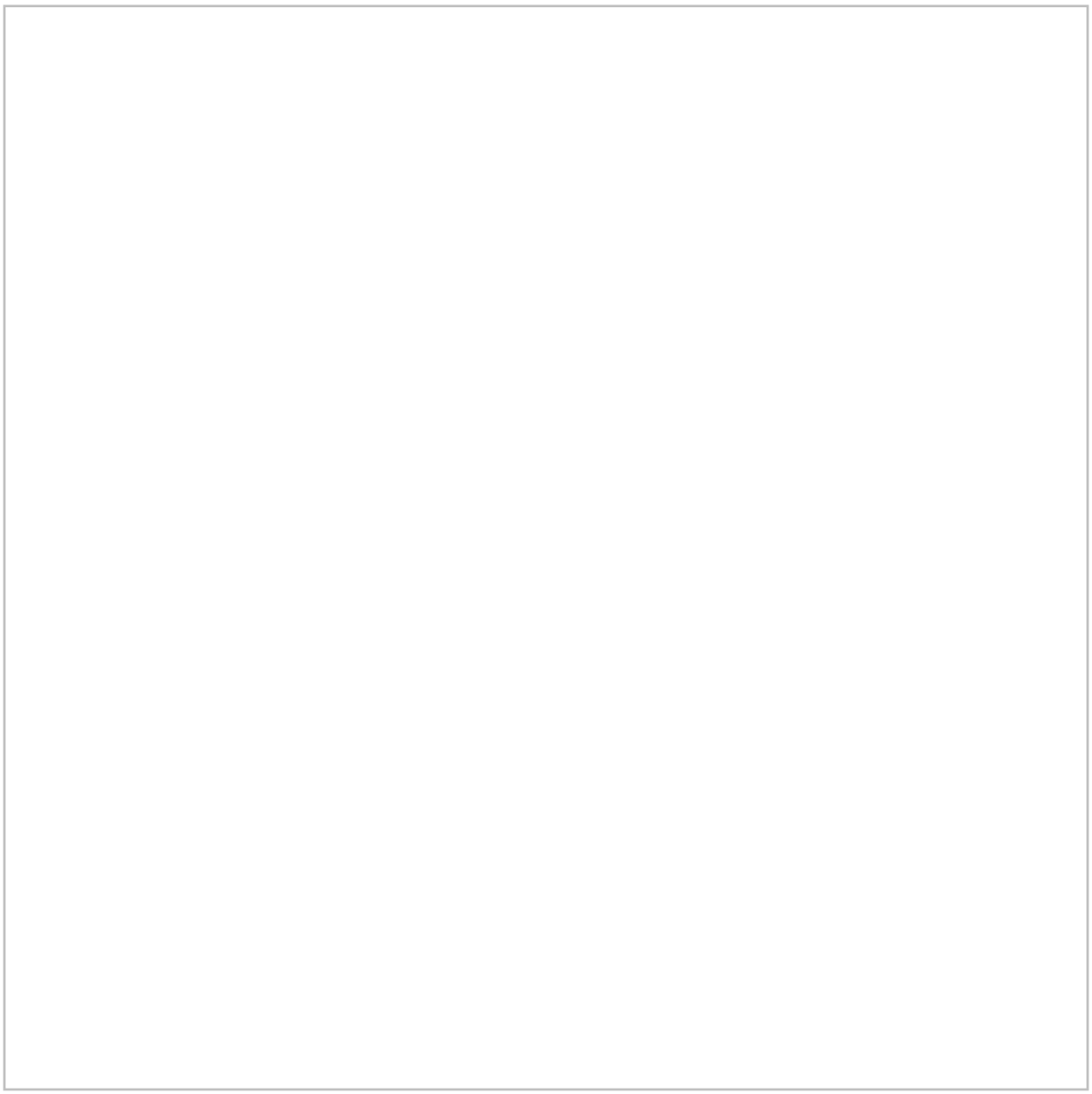
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Cote, Matthew (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:55:17 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.





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

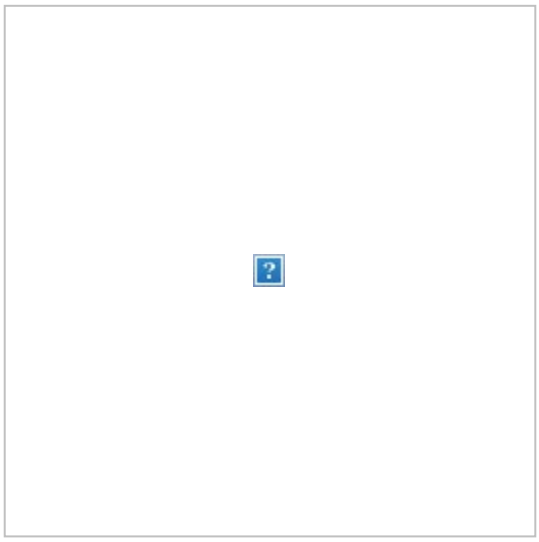
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Julce, Michael (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:55:17 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.



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

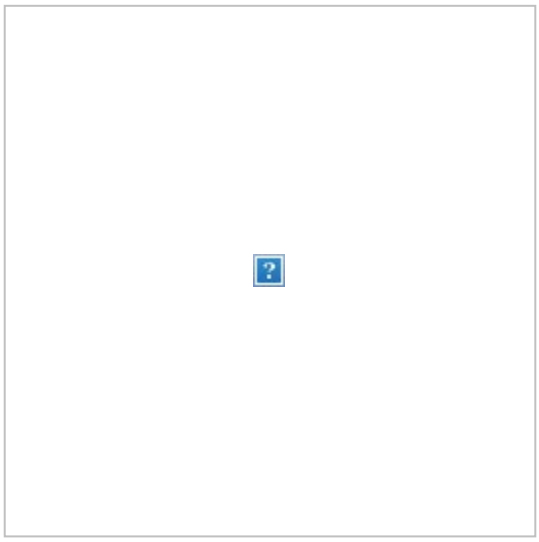
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Dunphy, David (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:55:16 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.



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

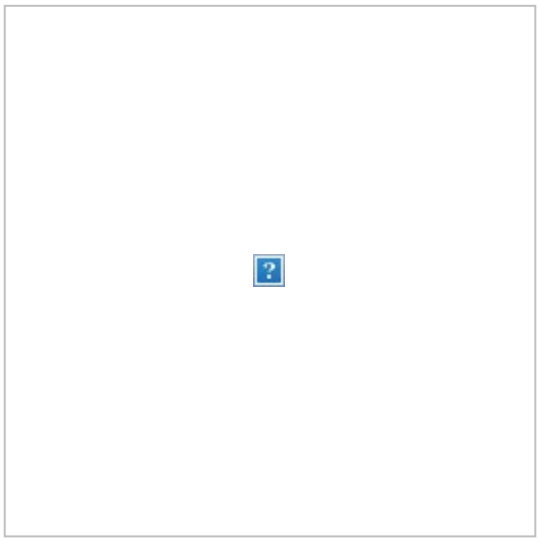
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Breton, Benjamin (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:55:15 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.



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

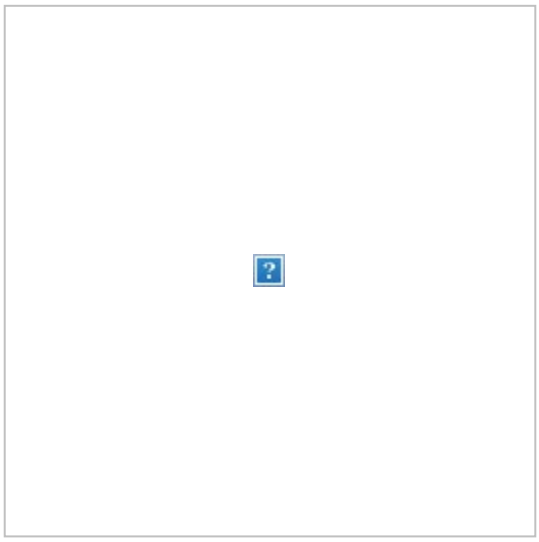
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Sanchez, Jorge (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:55:14 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.



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

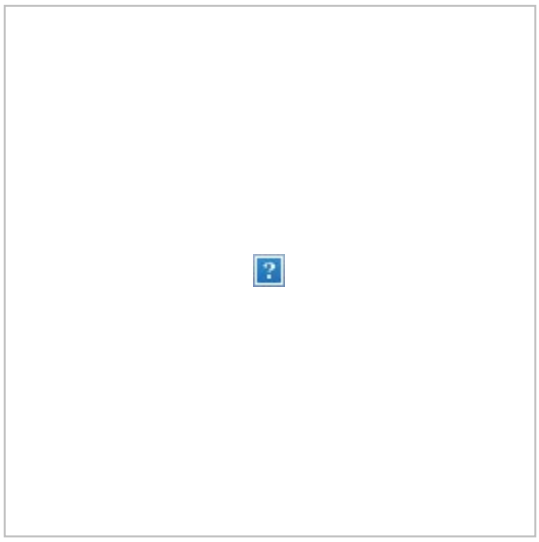
For more information on FINDER visit their website or contact them today!.

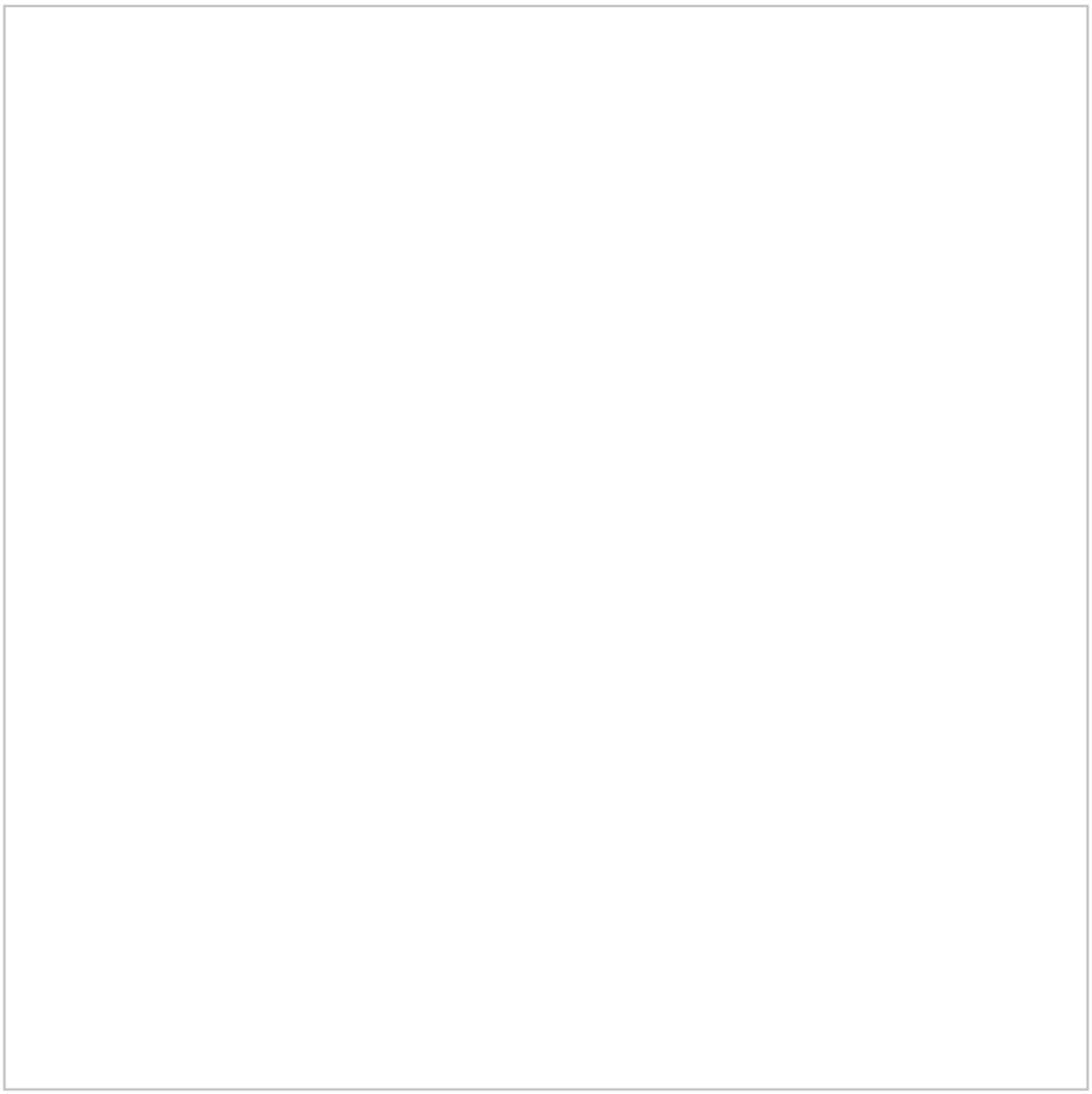
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Vath, Alexander (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:55:13 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.





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

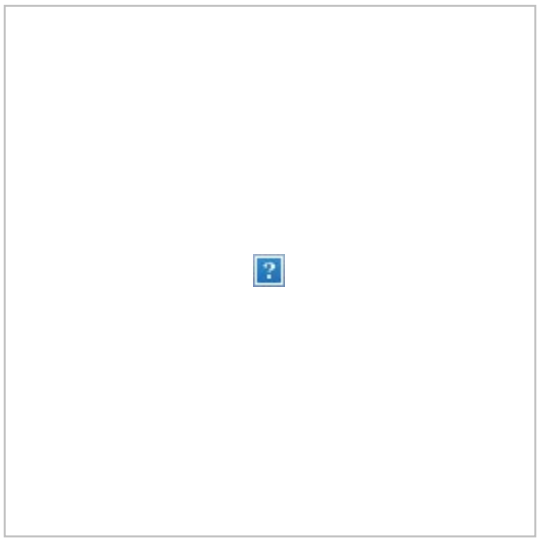
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Degisi, Costantino (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:55:13 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.



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

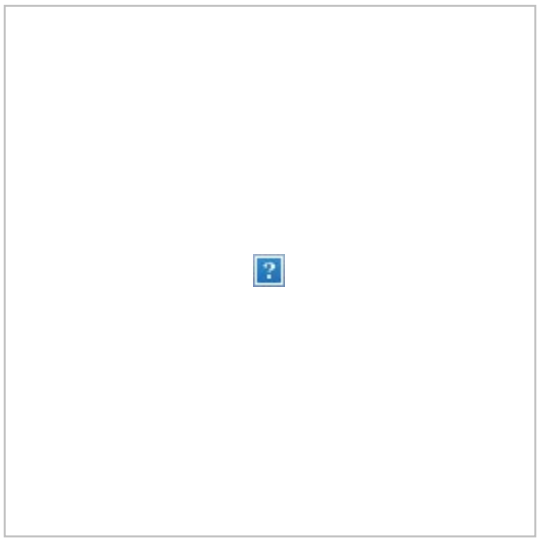
For more information on FINDER visit their website or contact them today!.

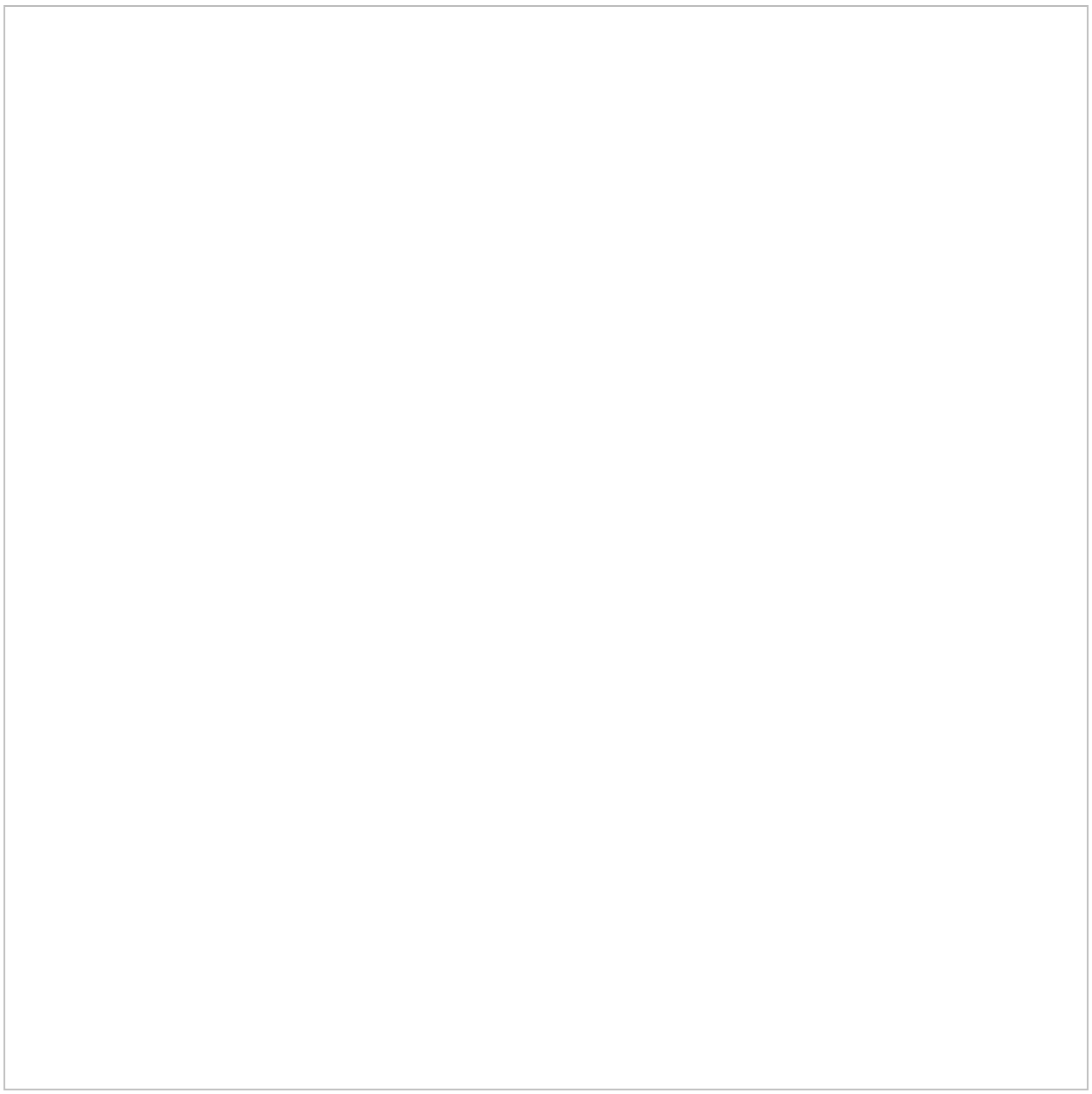
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Ortiz, Cameron (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:55:11 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.





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

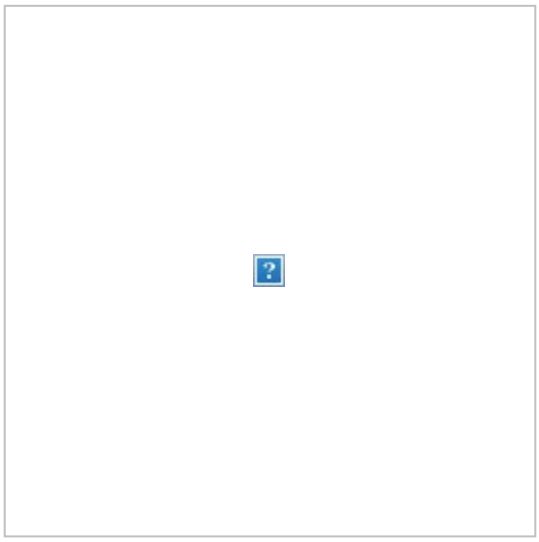
For more information on FINDER visit their website or contact them today!.

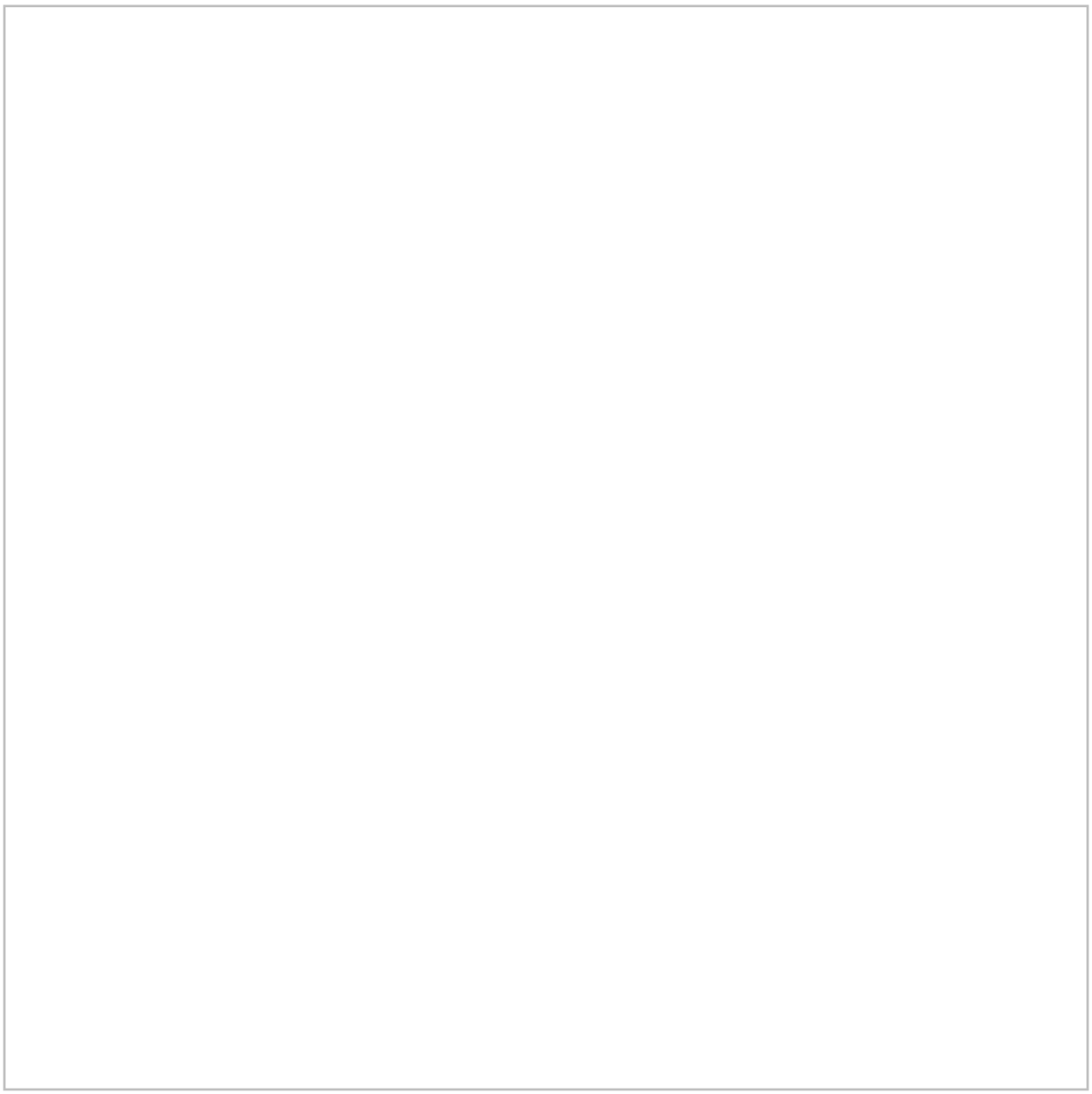
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Sullivan, Michael R (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:55:11 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.





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

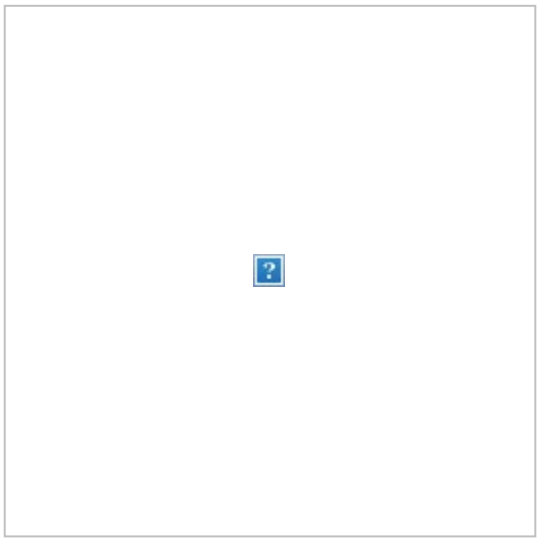
For more information on FINDER visit their website or contact them today!.

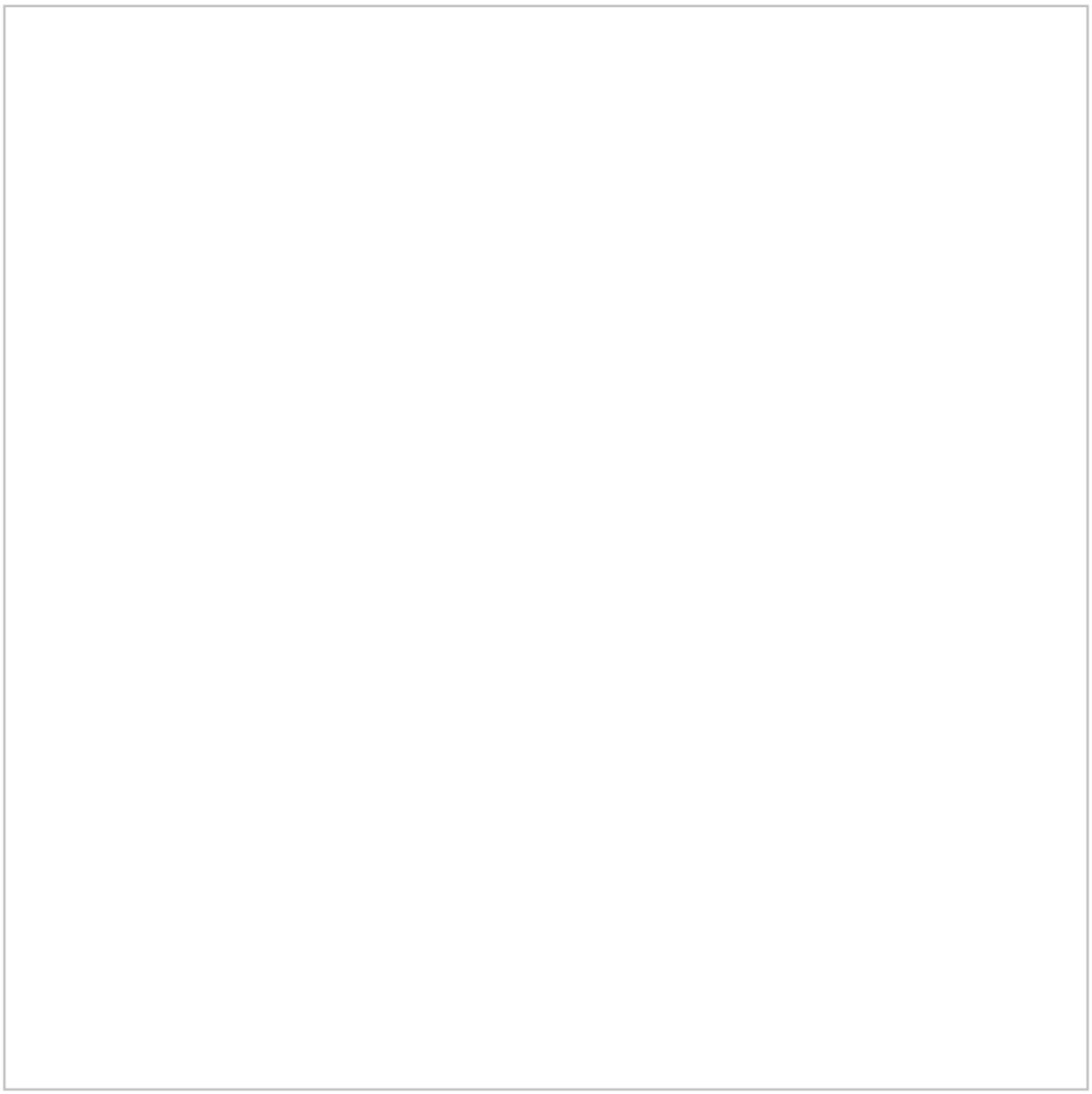
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Sandoval, Juan (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:45:39 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.





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

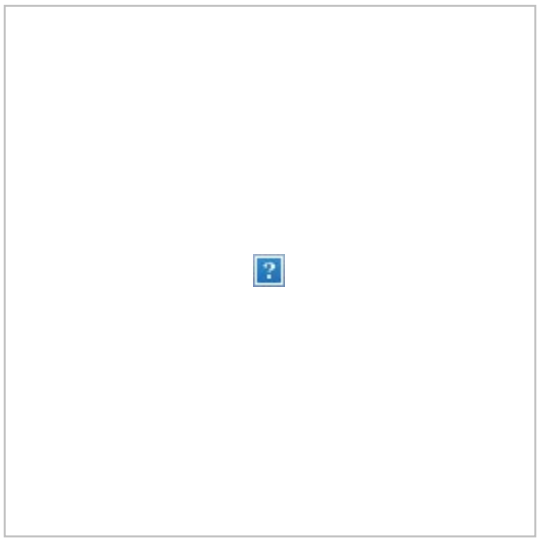
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Murgo, Christopher (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:45:31 PM

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



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

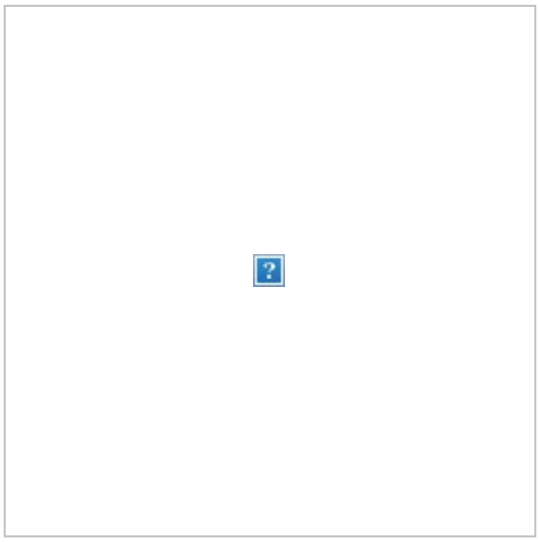
For more information on FINDER visit their website or contact them today!.

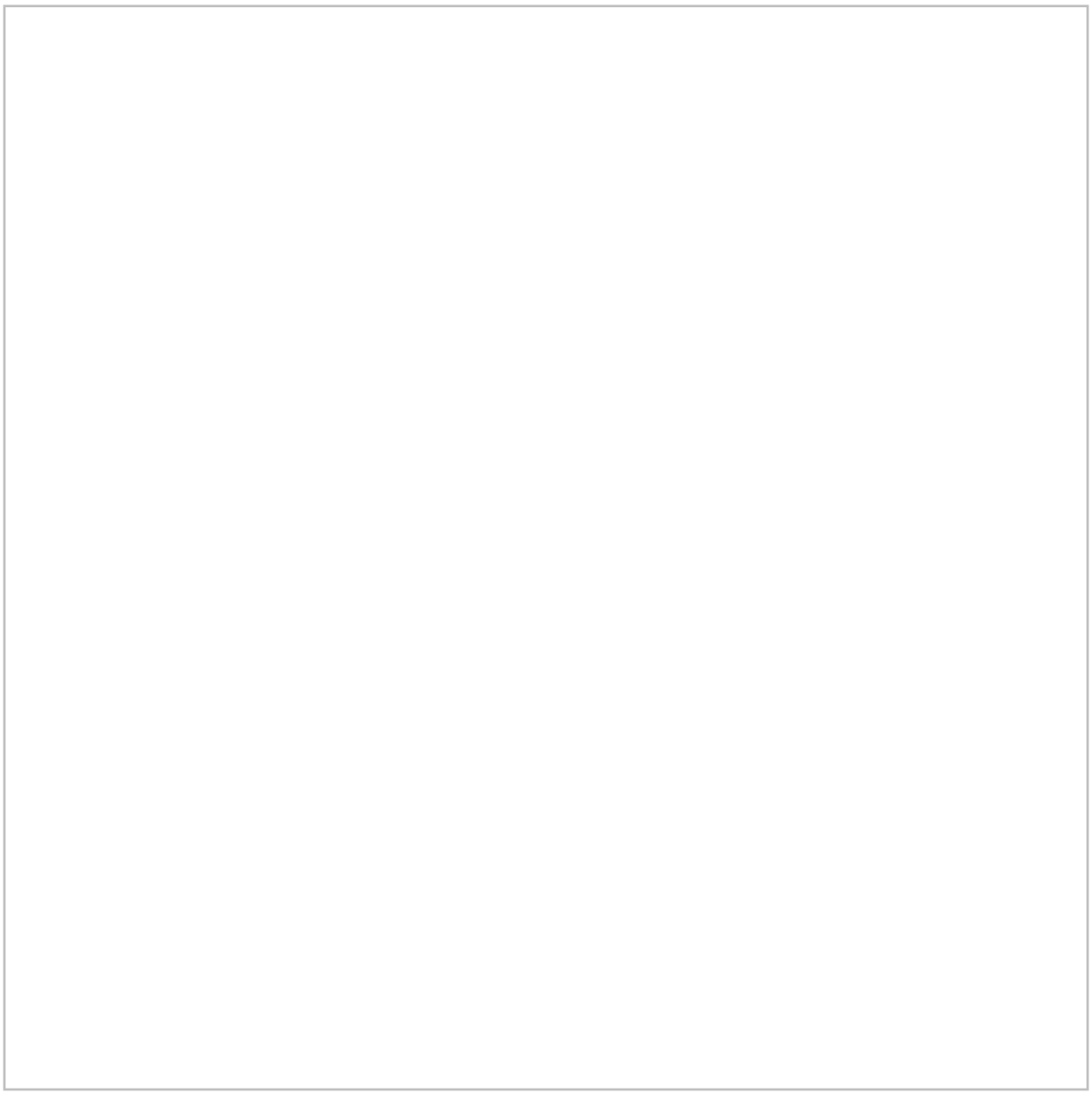
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: O"Keefe, Patrick R (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:45:31 PM

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





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

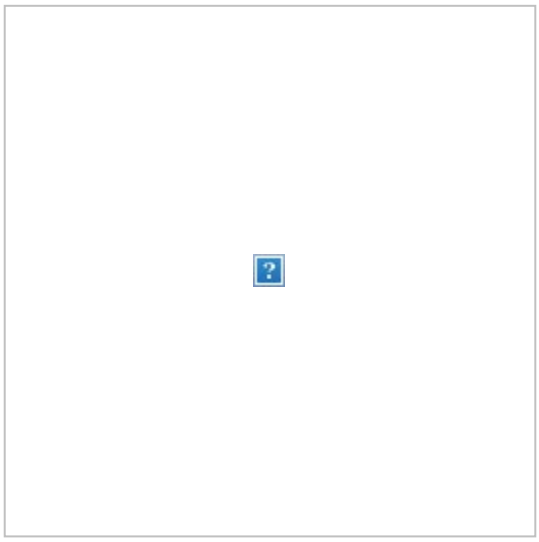
For more information on FINDER visit their website or contact them today!.

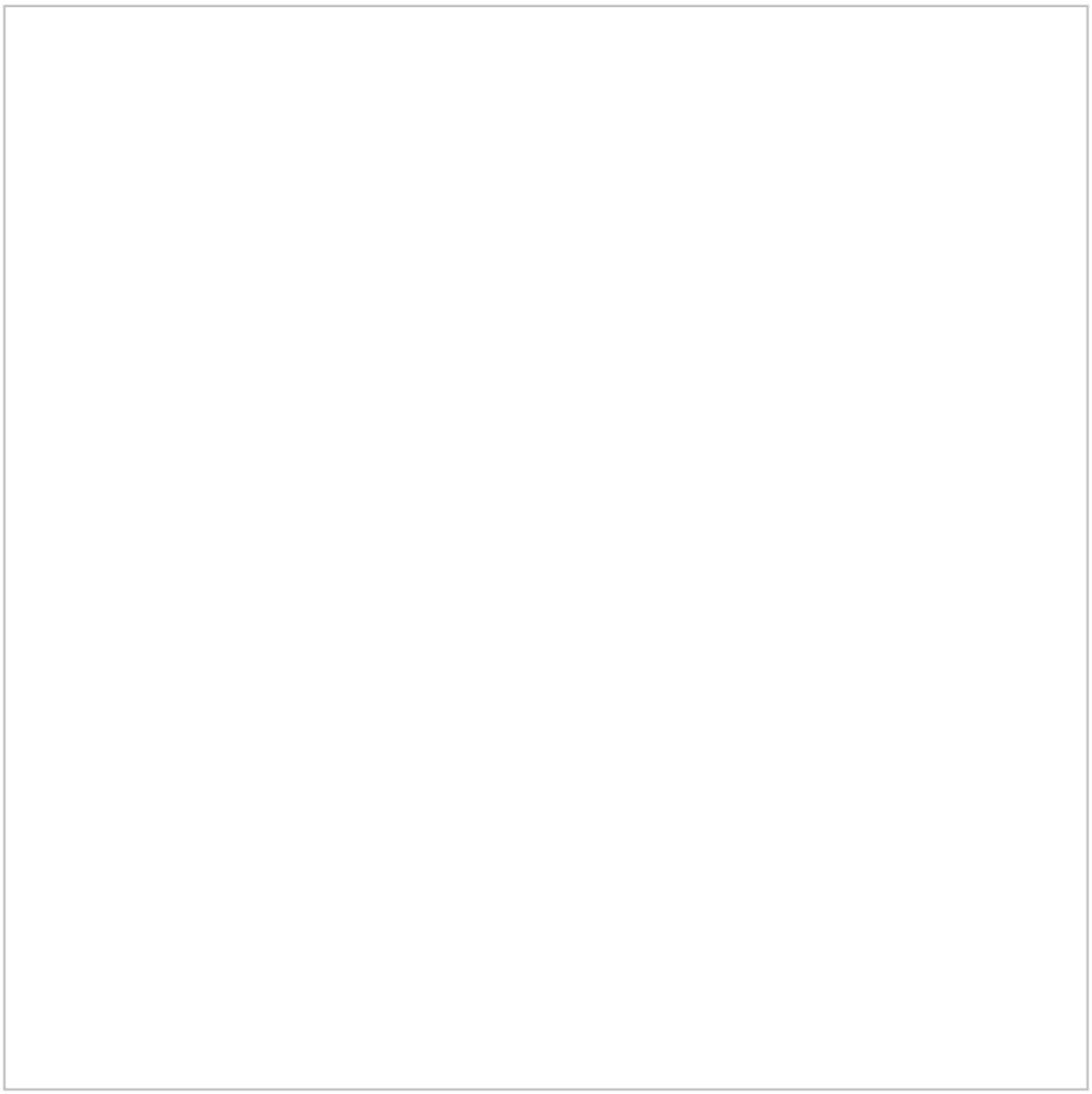
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Donnini, Nicholas (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:45:30 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.





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

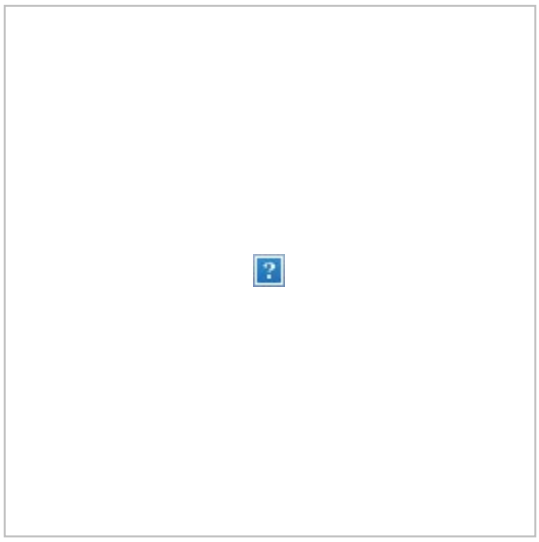
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Deady, Sean (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:45:29 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.



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

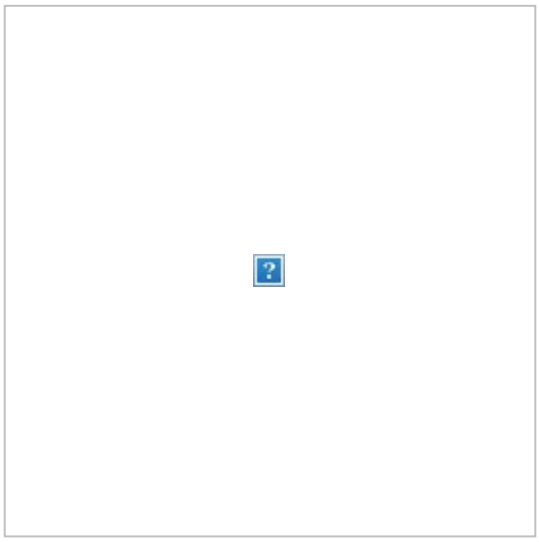
For more information on FINDER visit their website or contact them today!.

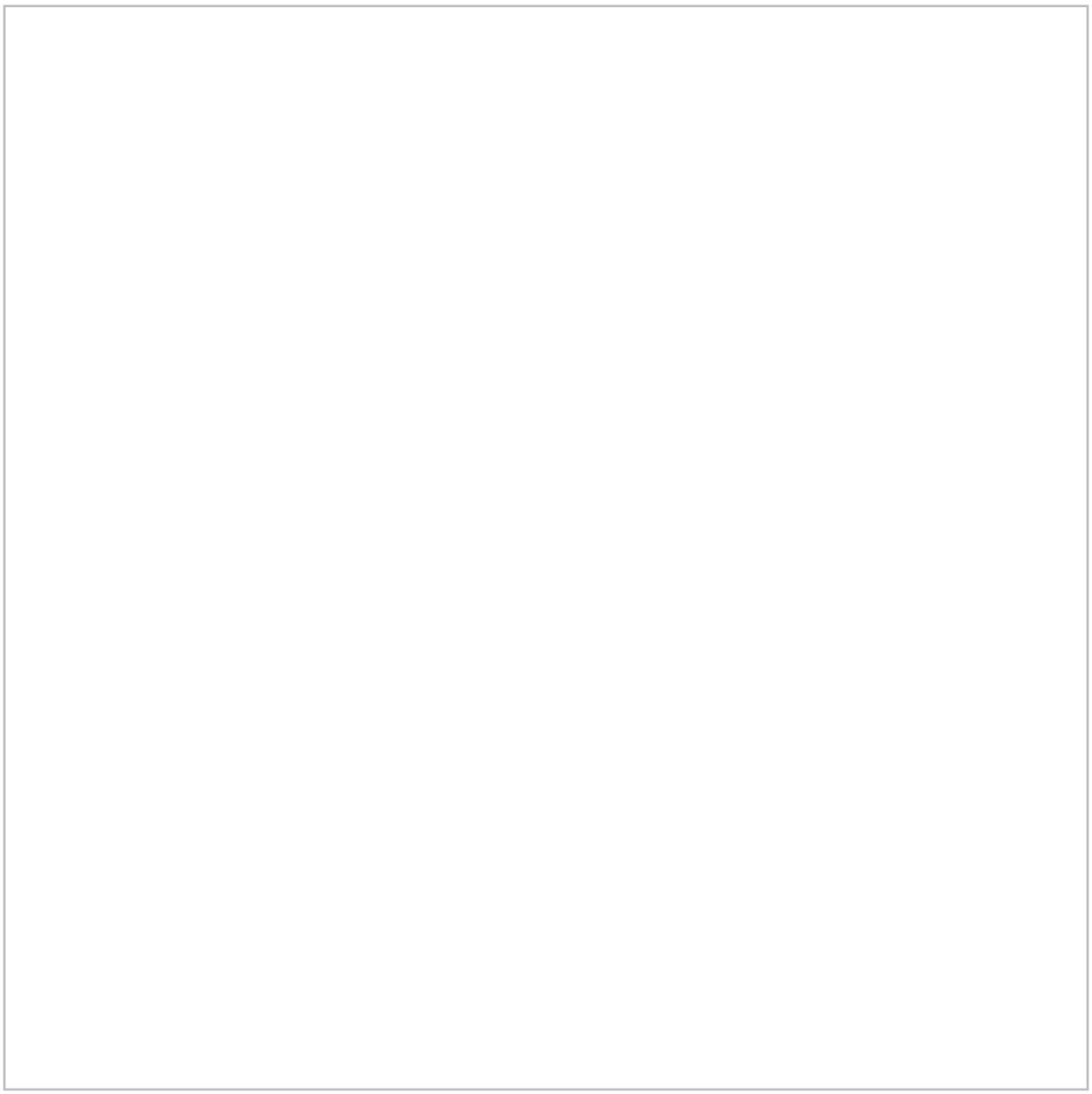
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Torres, Francis (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:45:28 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.





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

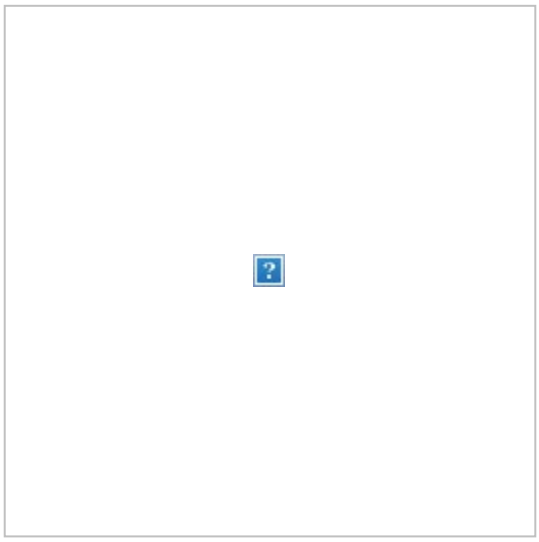
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: zzLannon, John (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:45:16 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.



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

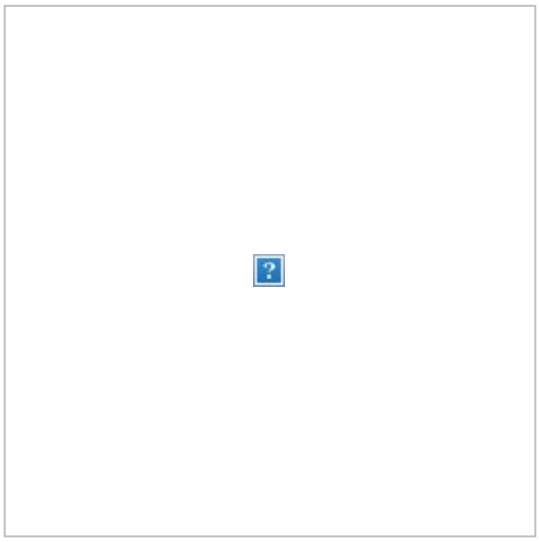
For more information on FINDER visit their website or contact them today!.

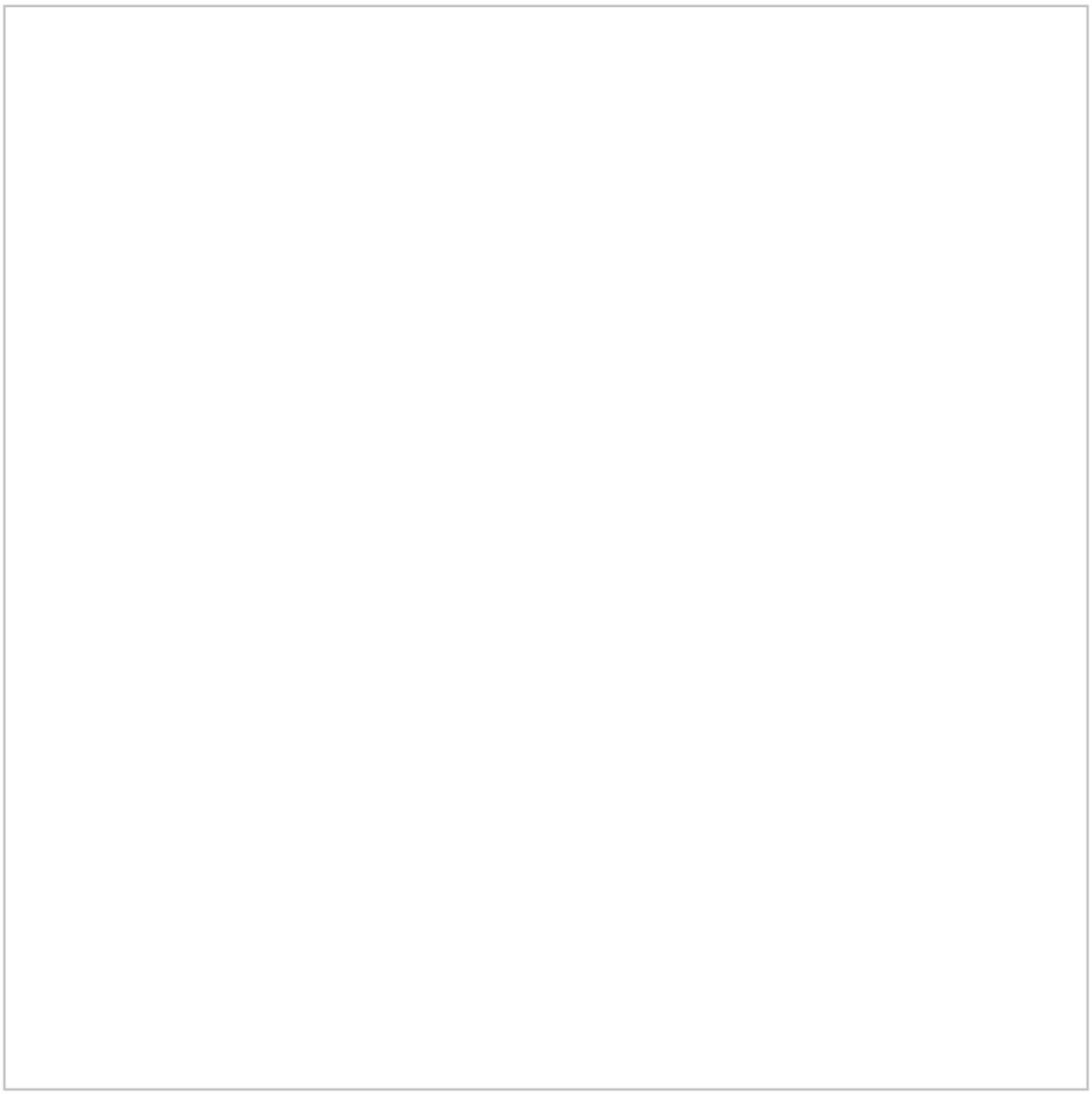
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Smith, Alexander (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:45:16 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.





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

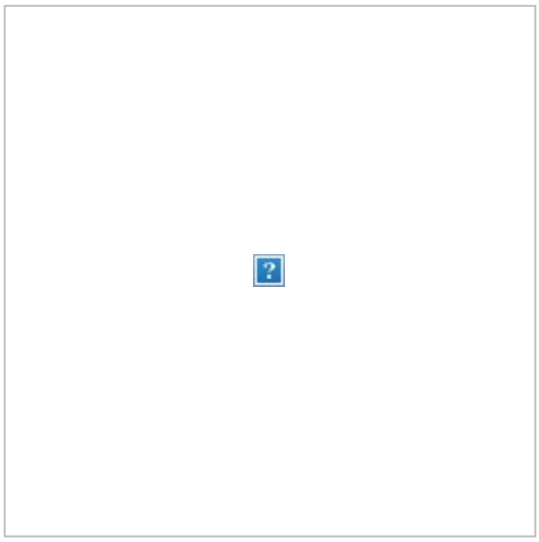
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Williams, Louis (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:45:15 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.



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

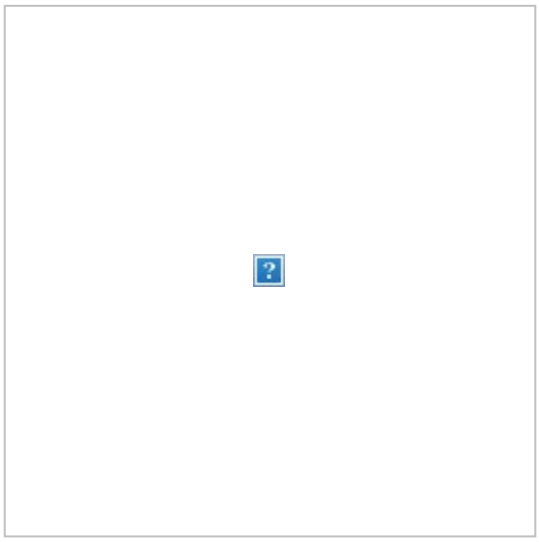
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Sherber, Peter (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:45:14 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.



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

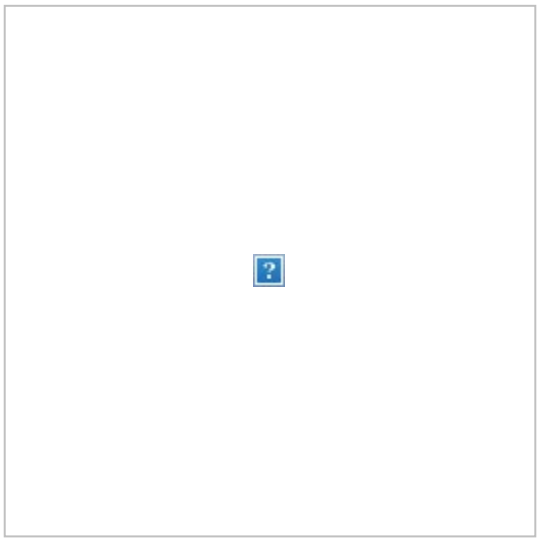
For more information on FINDER visit their website or contact them today!.

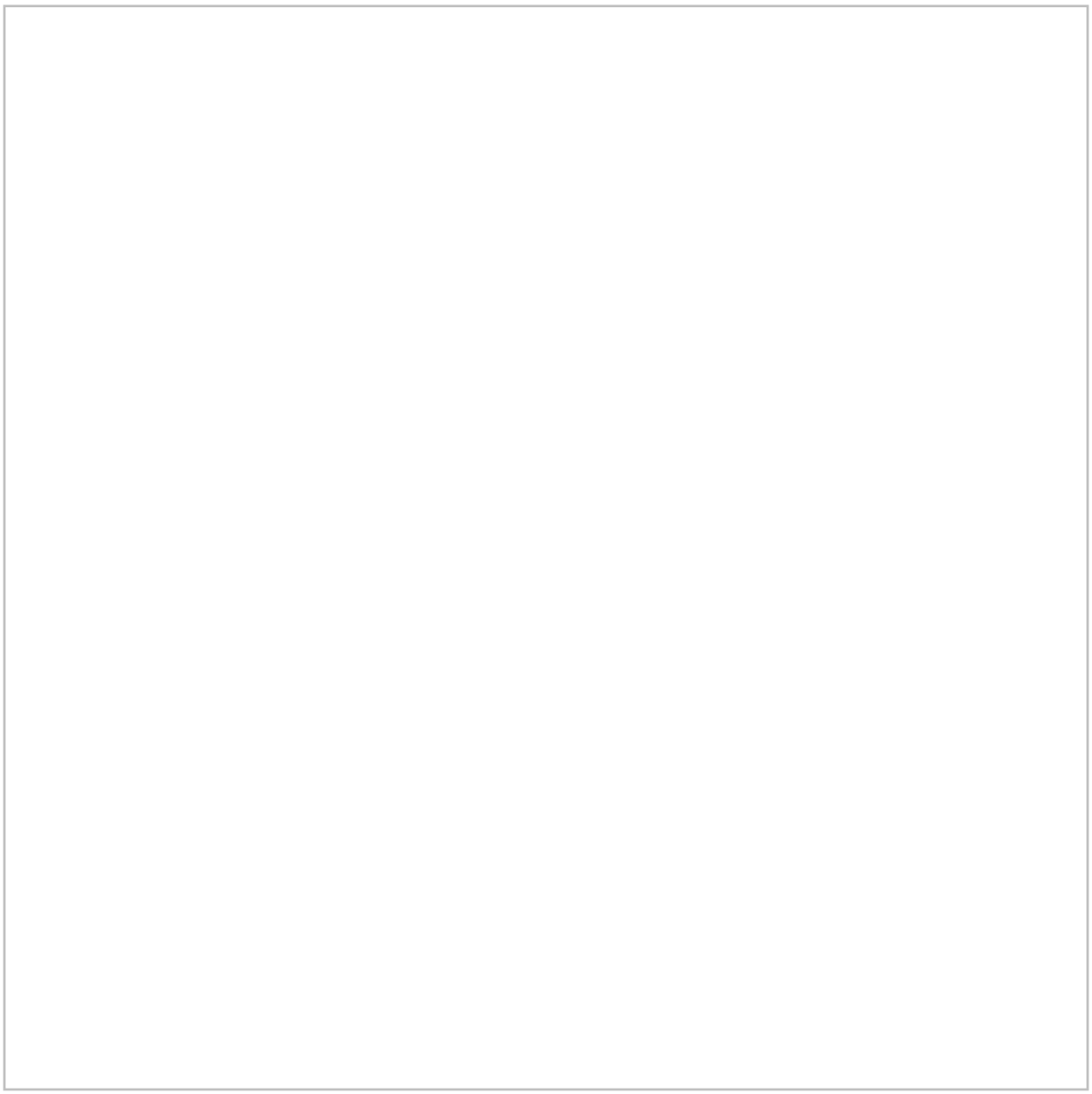
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Carnes, Brendan A (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:45:14 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.





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

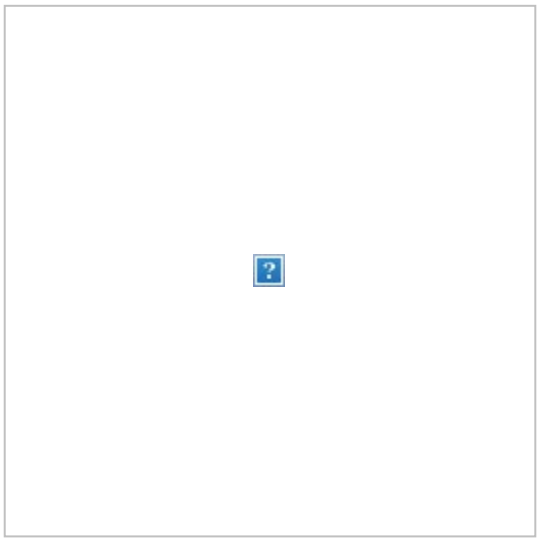
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Collett, Joseph (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:32:50 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.



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

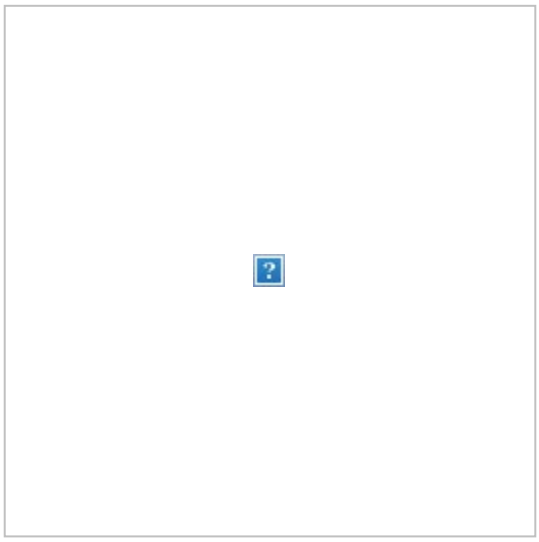
For more information on FINDER visit their website or contact them today!.

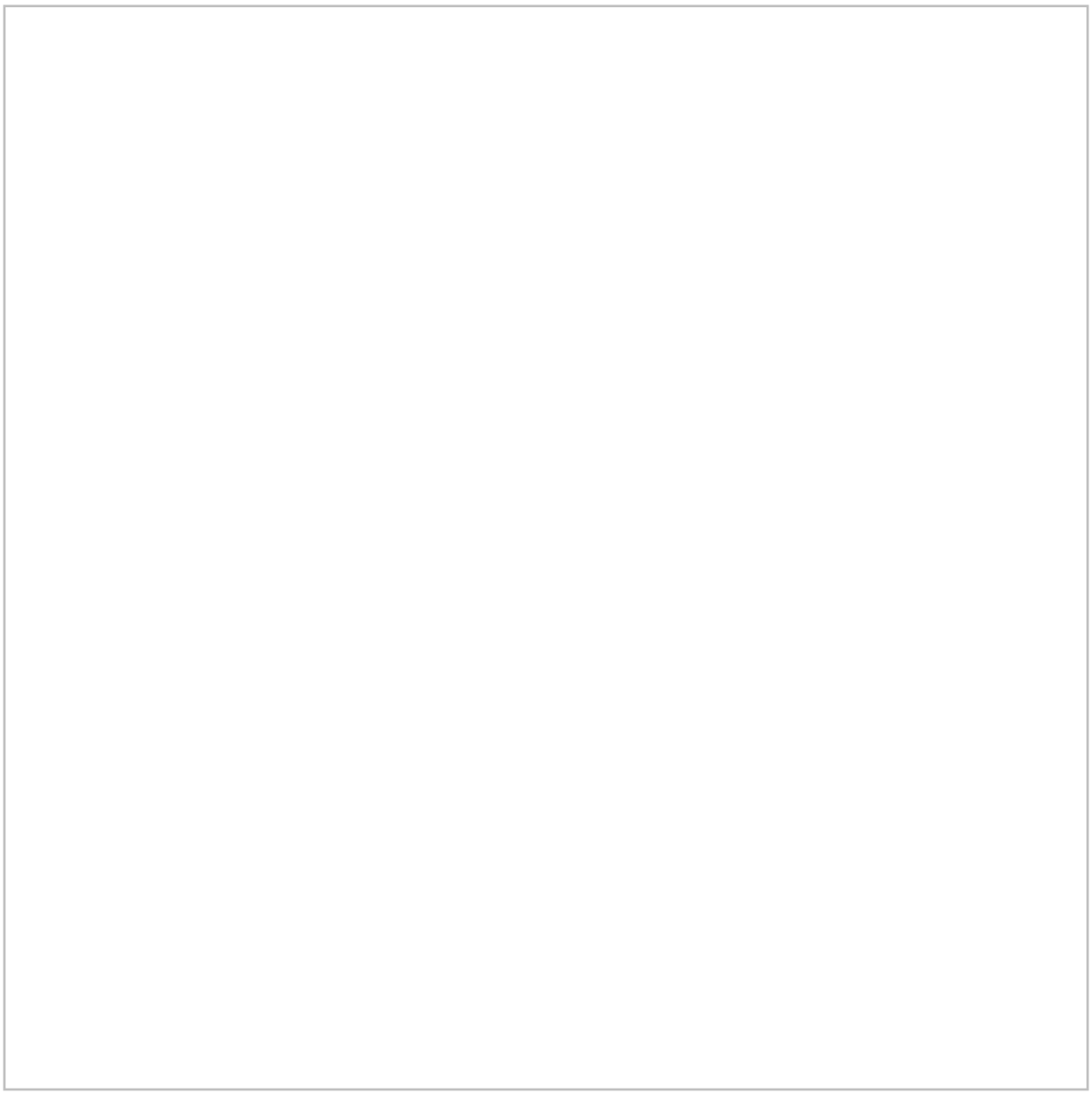
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Gately, Cali (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:32:48 PM

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





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

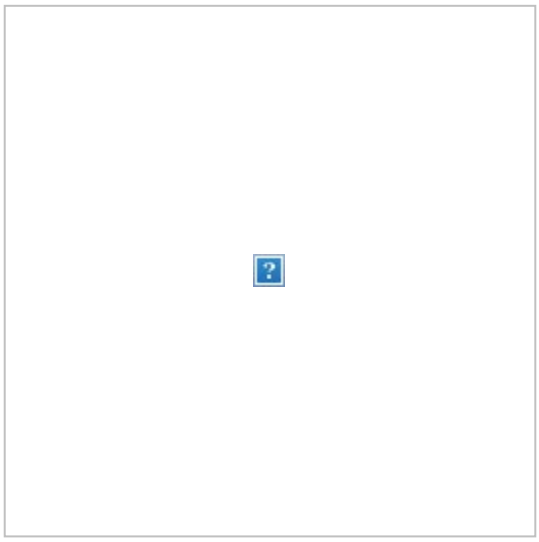
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Harrington, Daniel J (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:32:47 PM

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



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

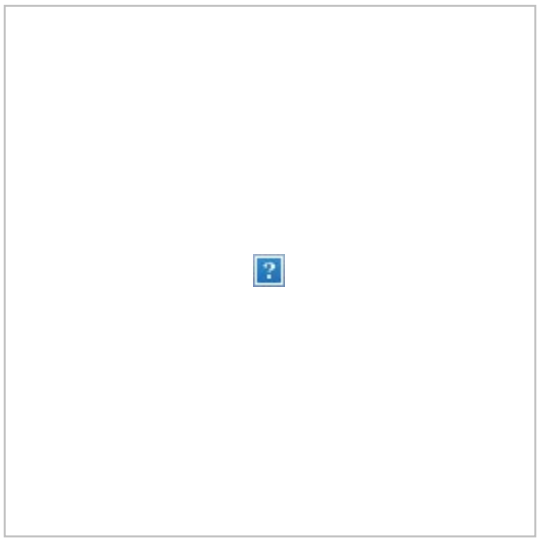
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: McCarthy, Jay (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:32:45 PM

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



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

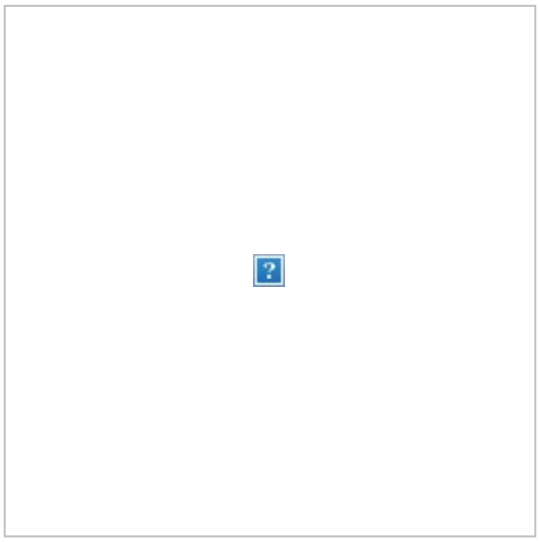
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Hinchion, Daniel L (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:32:42 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.



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

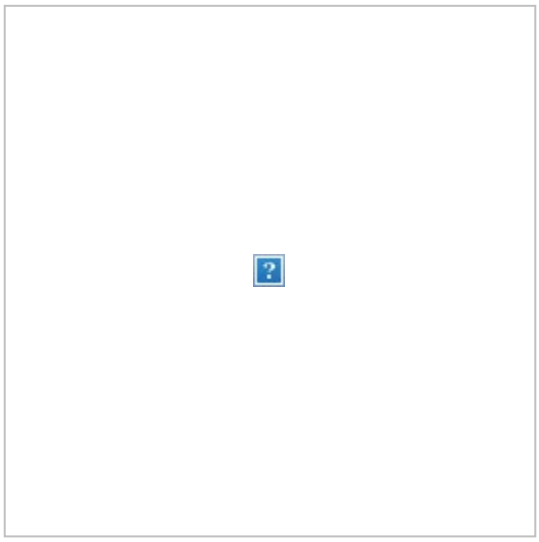
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Mccrave, Patrick (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:32:40 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.



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

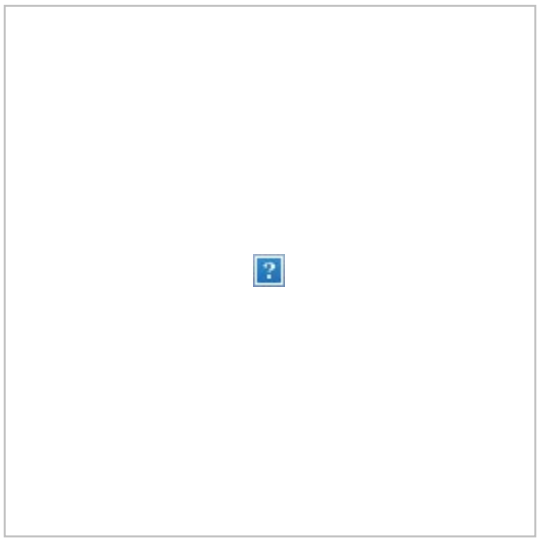
For more information on FINDER visit their website or contact them today!.

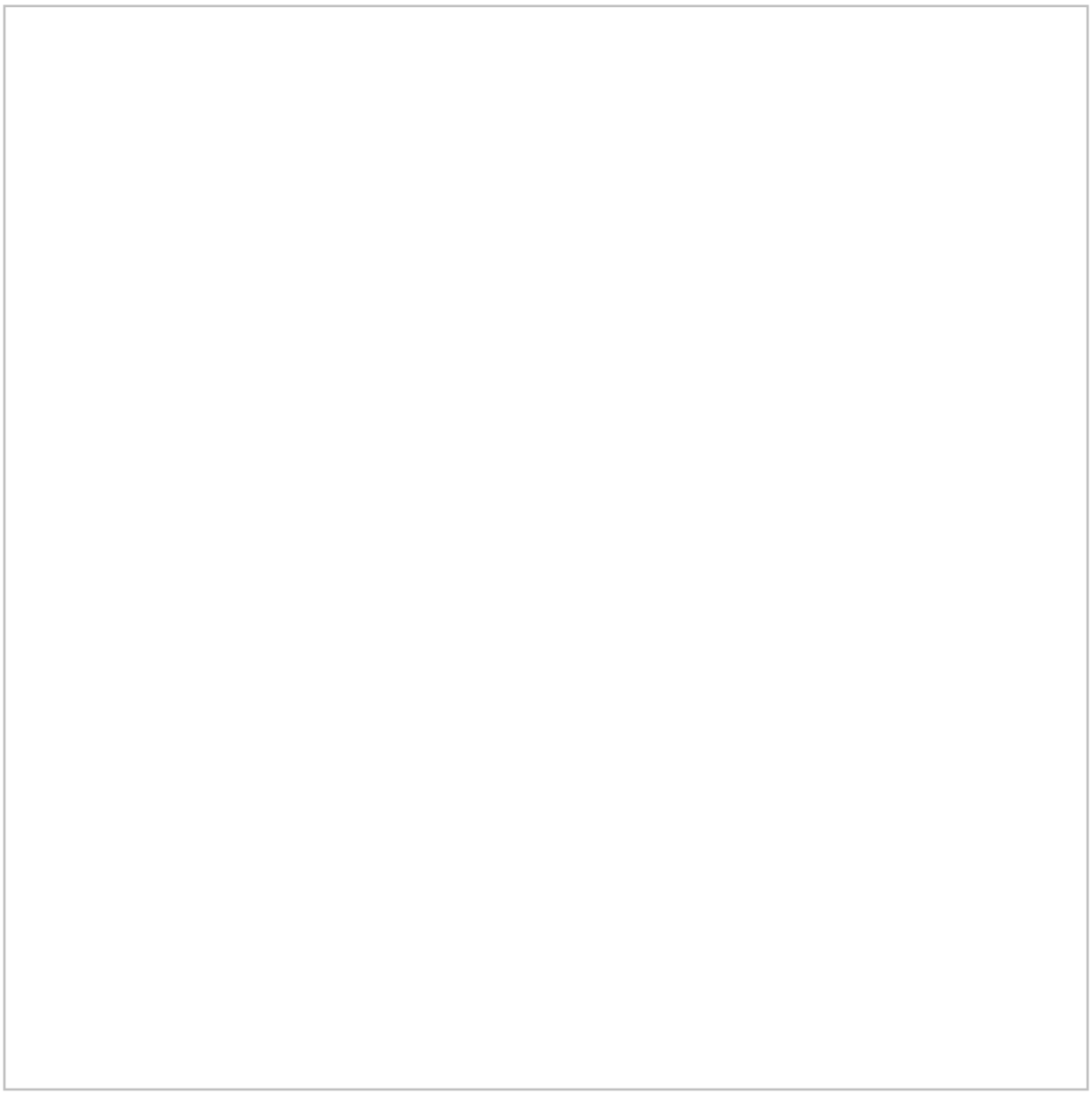
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: McStay, Patrick (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:22:15 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.





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

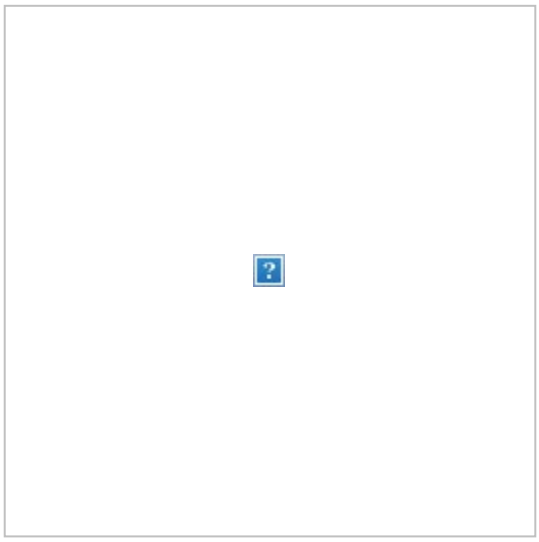
For more information on FINDER visit their website or contact them today!.

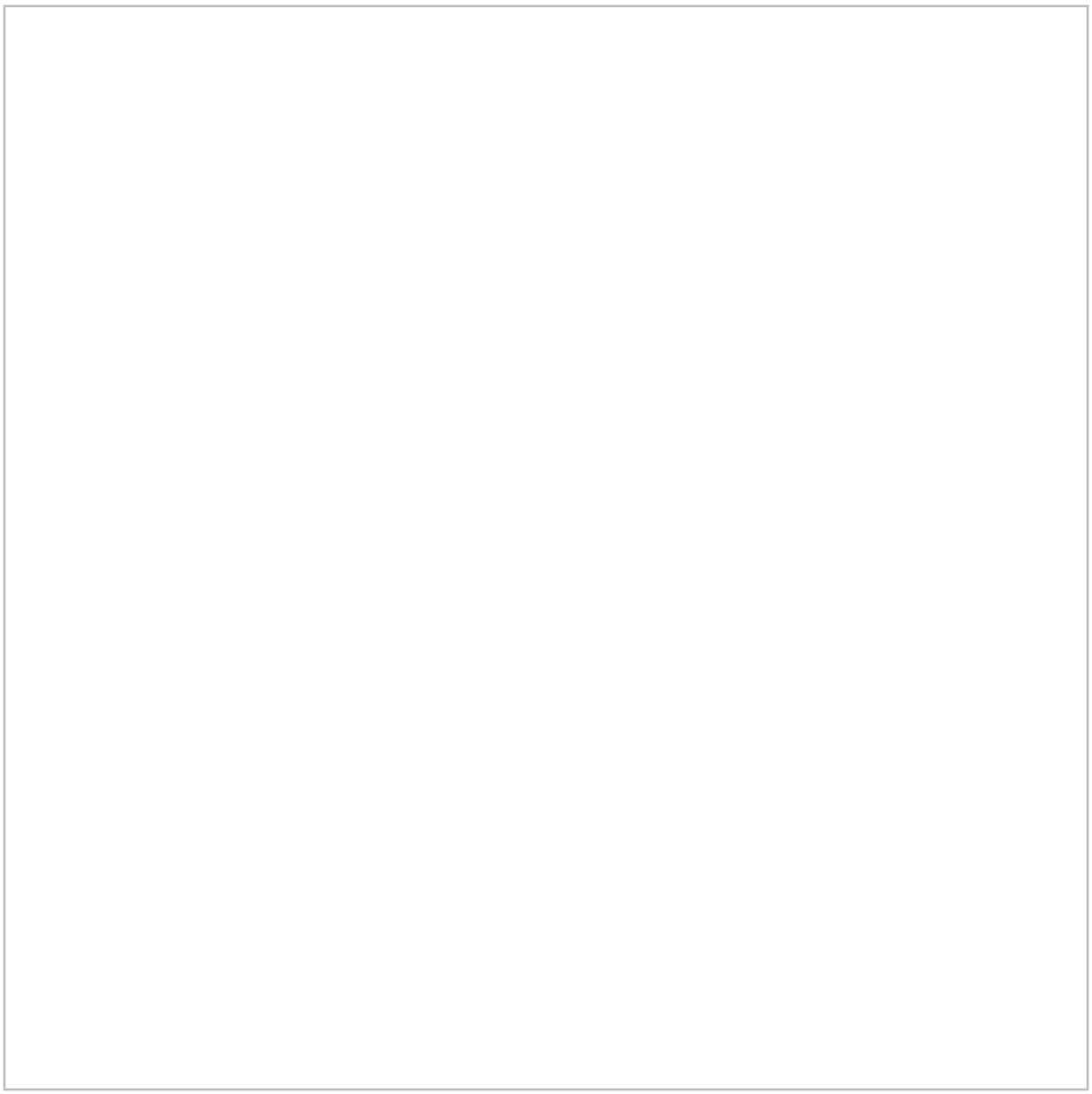
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Maxwell, Marshall D (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:22:15 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.





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

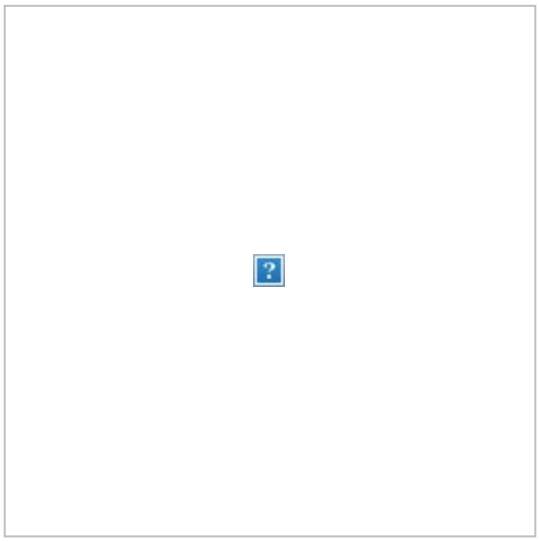
For more information on FINDER visit their website or contact them today!.

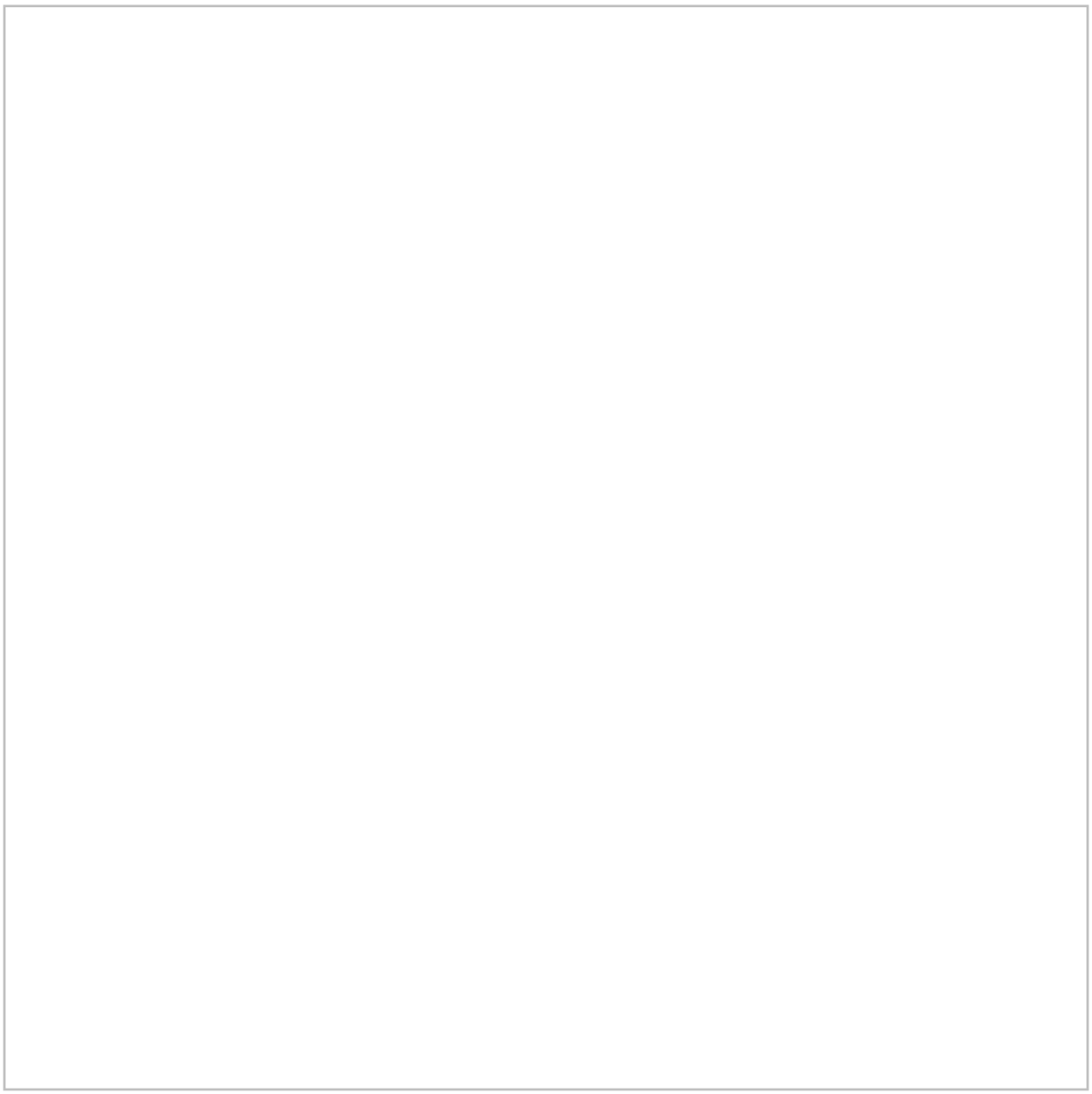
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Chalmers, Traylen (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:22:13 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.





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

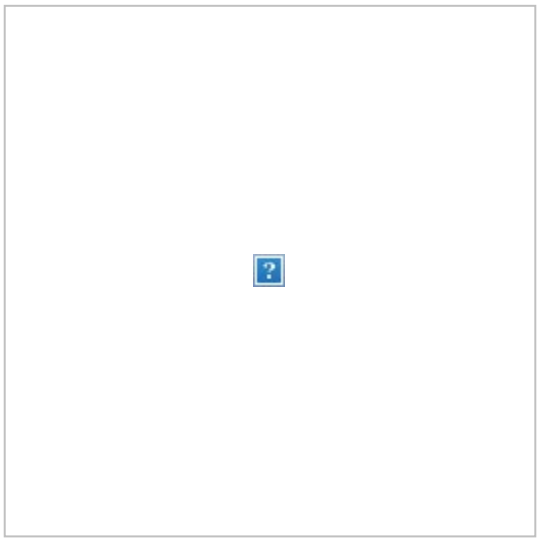
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Gately, Cali (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:12:35 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.



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

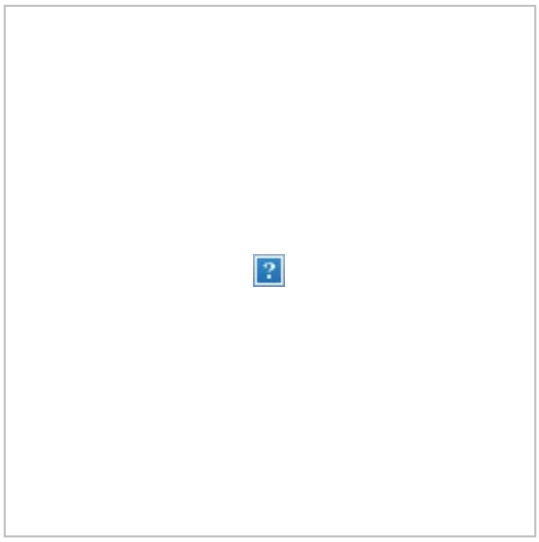
For more information on FINDER visit their website or contact them today!.

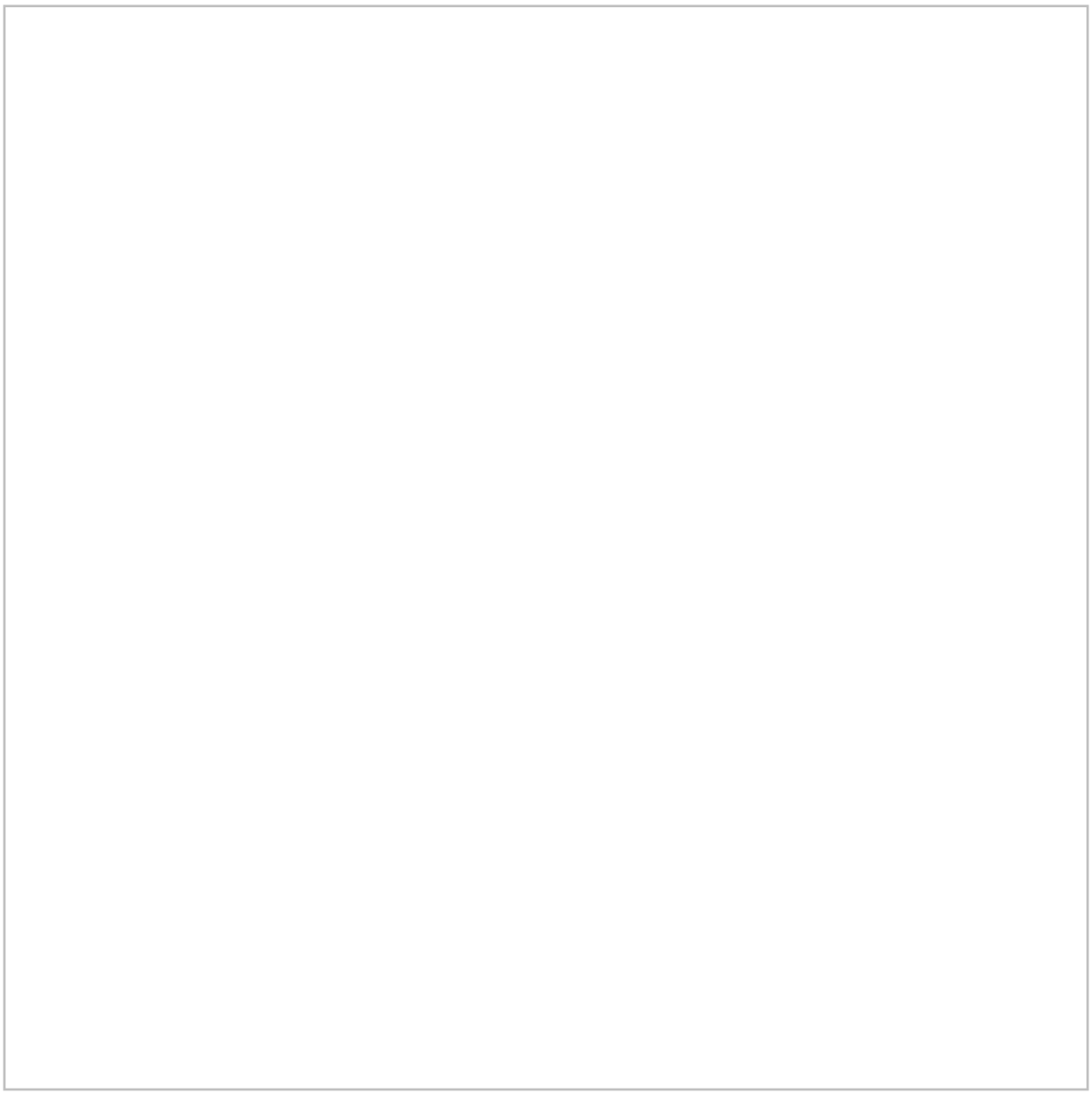
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Rego, Paul (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:12:30 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.





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

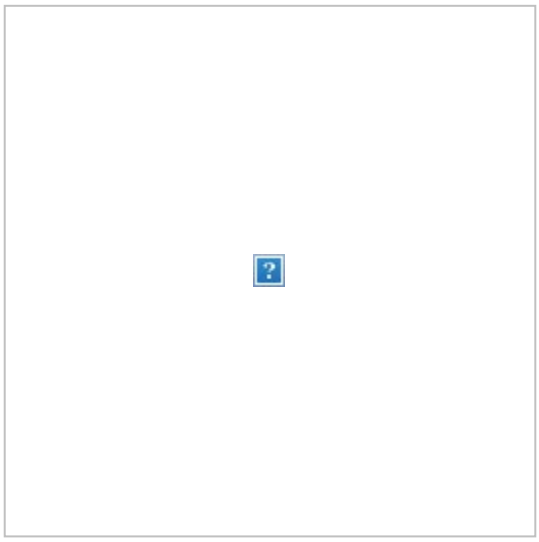
For more information on FINDER visit their website or contact them today!.

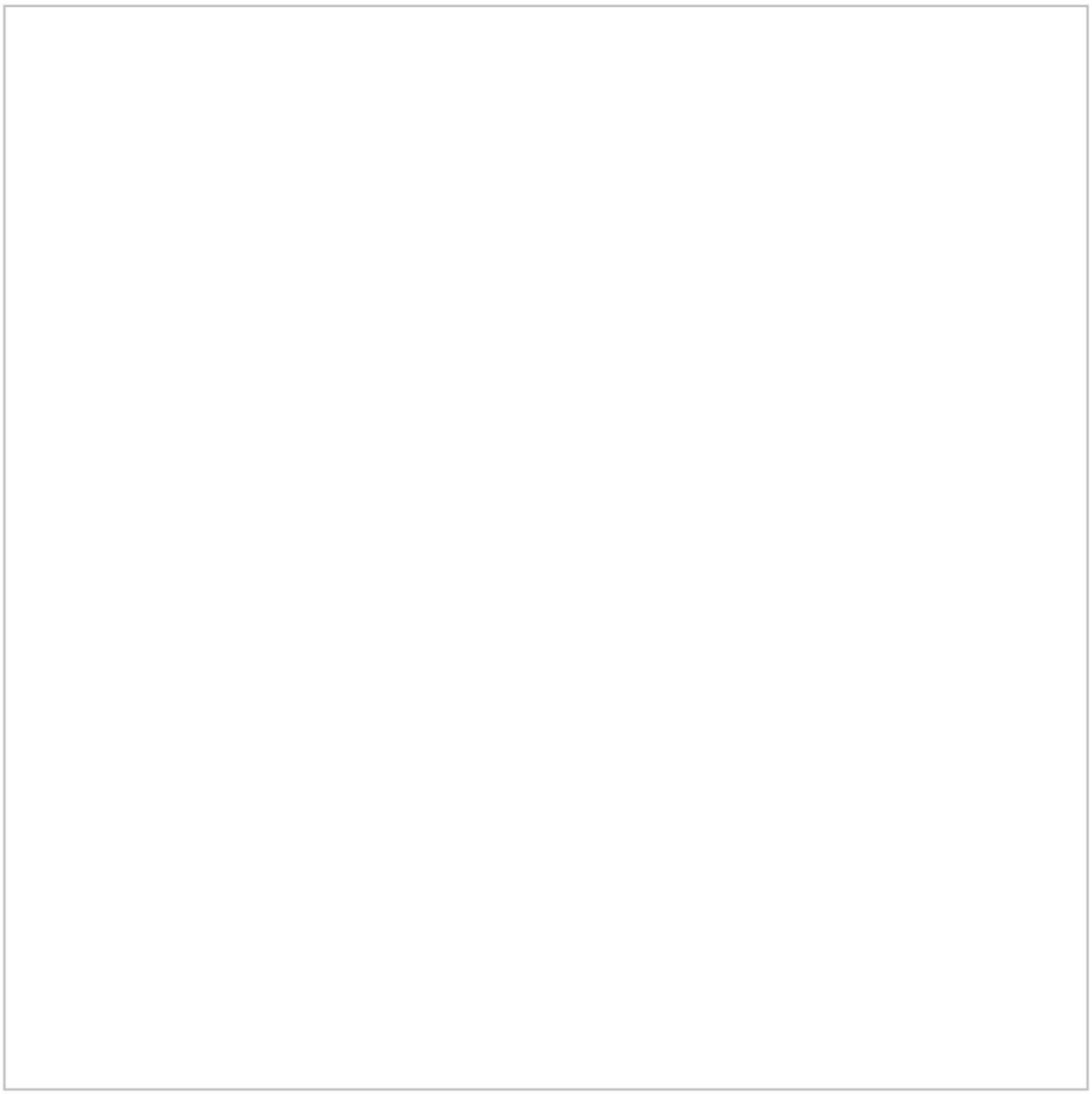
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Dimarzio, Michael (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:12:29 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.





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

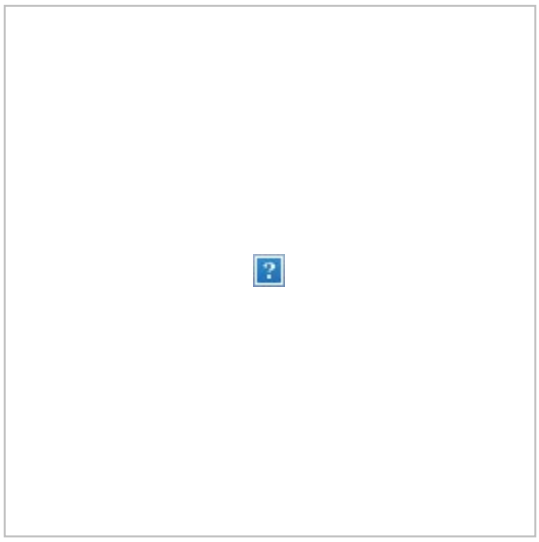
For more information on FINDER visit their website or contact them today!.

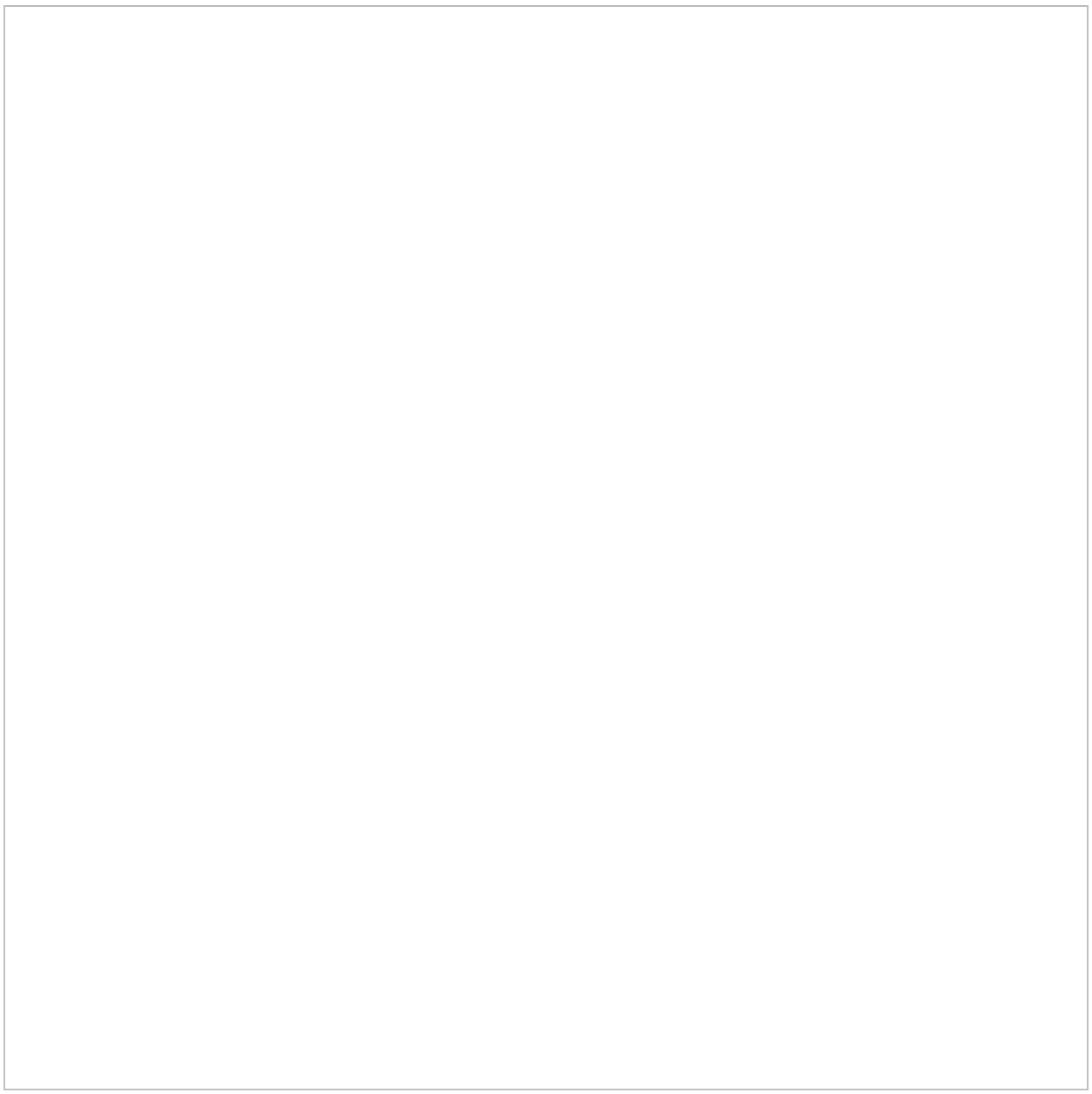
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Rabbitt, Joseph (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:12:29 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.





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

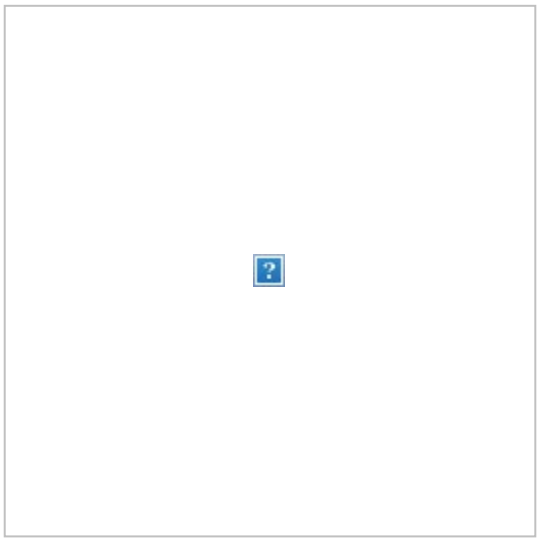
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Farley, Jay (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:12:27 PM

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



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

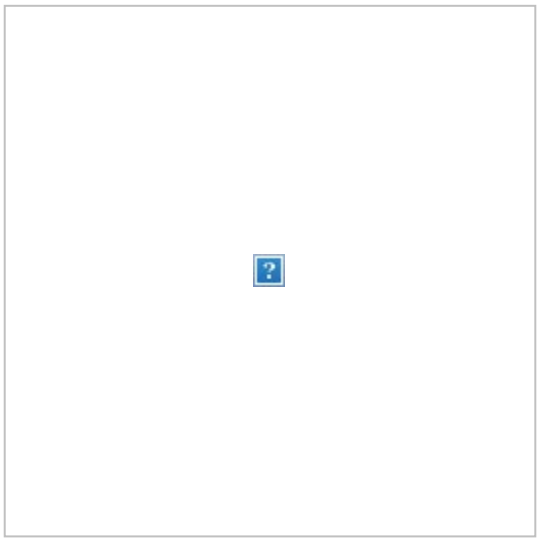
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Macdonald, Jerome (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:12:26 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.



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

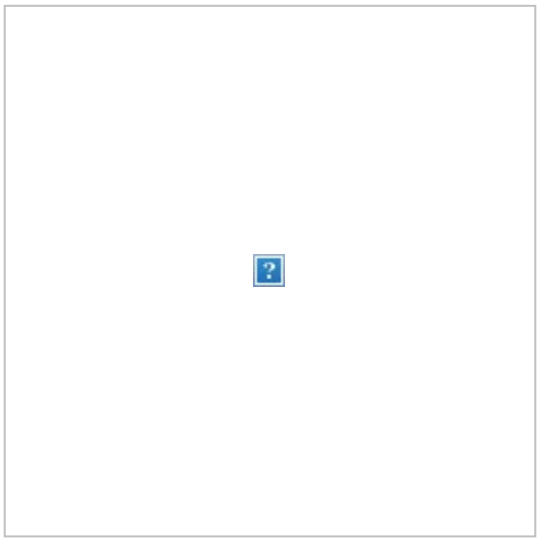
For more information on FINDER visit their website or contact them today!.

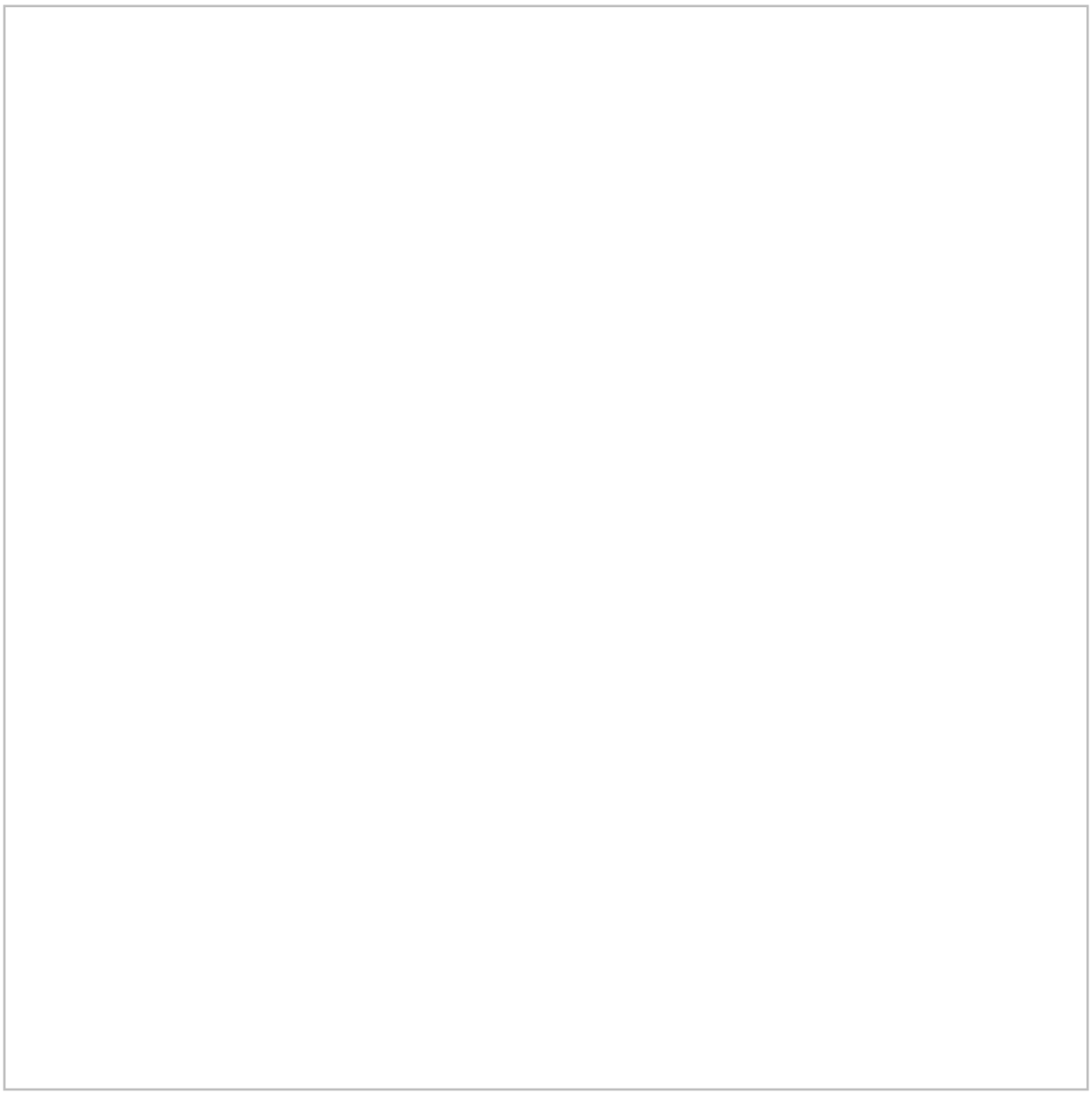
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Macdonald, Michael (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:12:21 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.





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

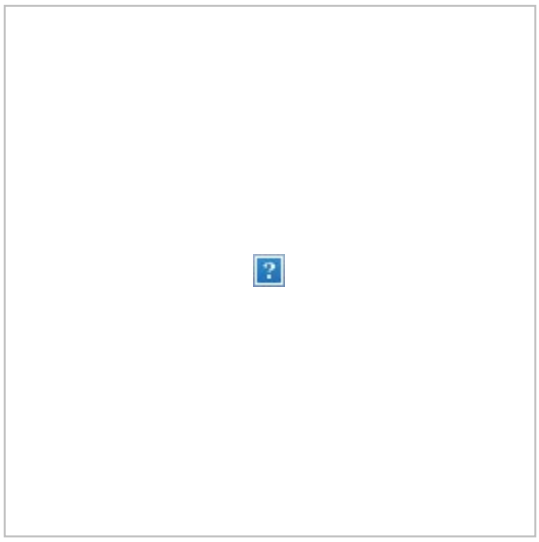
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Ryan, Michael K (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:12:18 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.



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

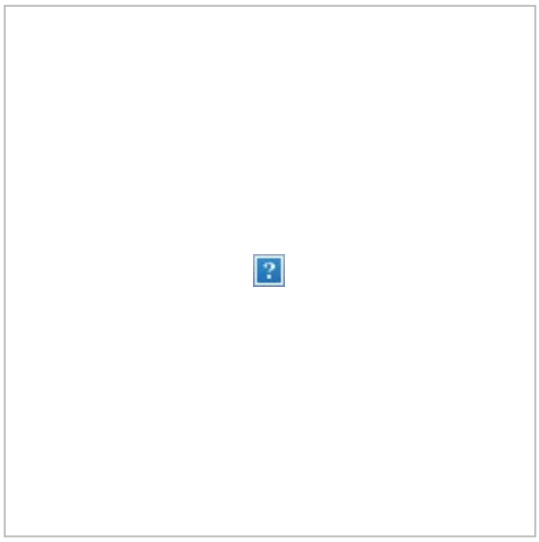
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Mcnamara, Patrick (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:12:18 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.



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

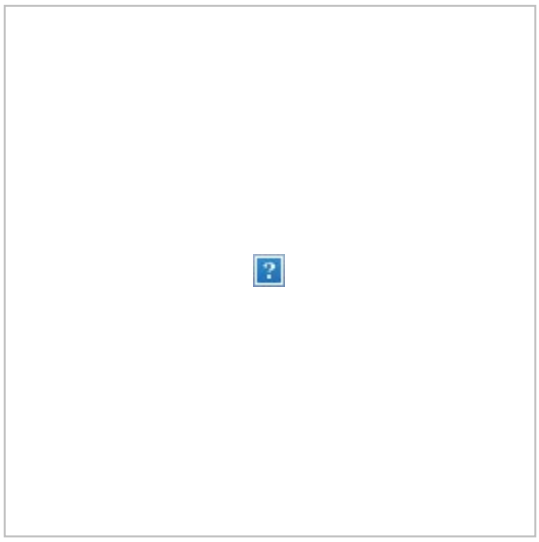
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Kent, Michael G. (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:12:17 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.



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

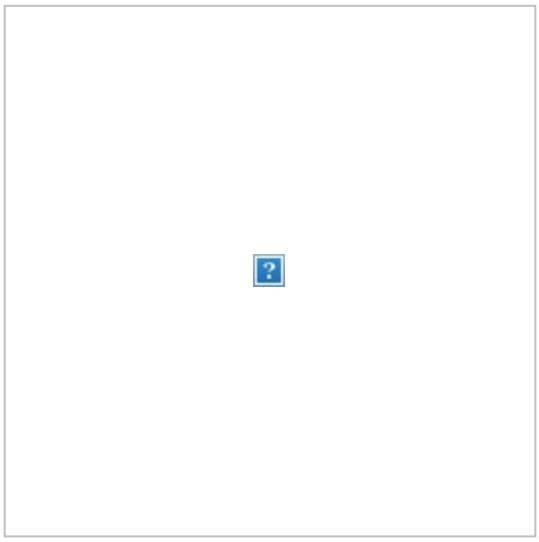
For more information on FINDER visit their website or contact them today!.

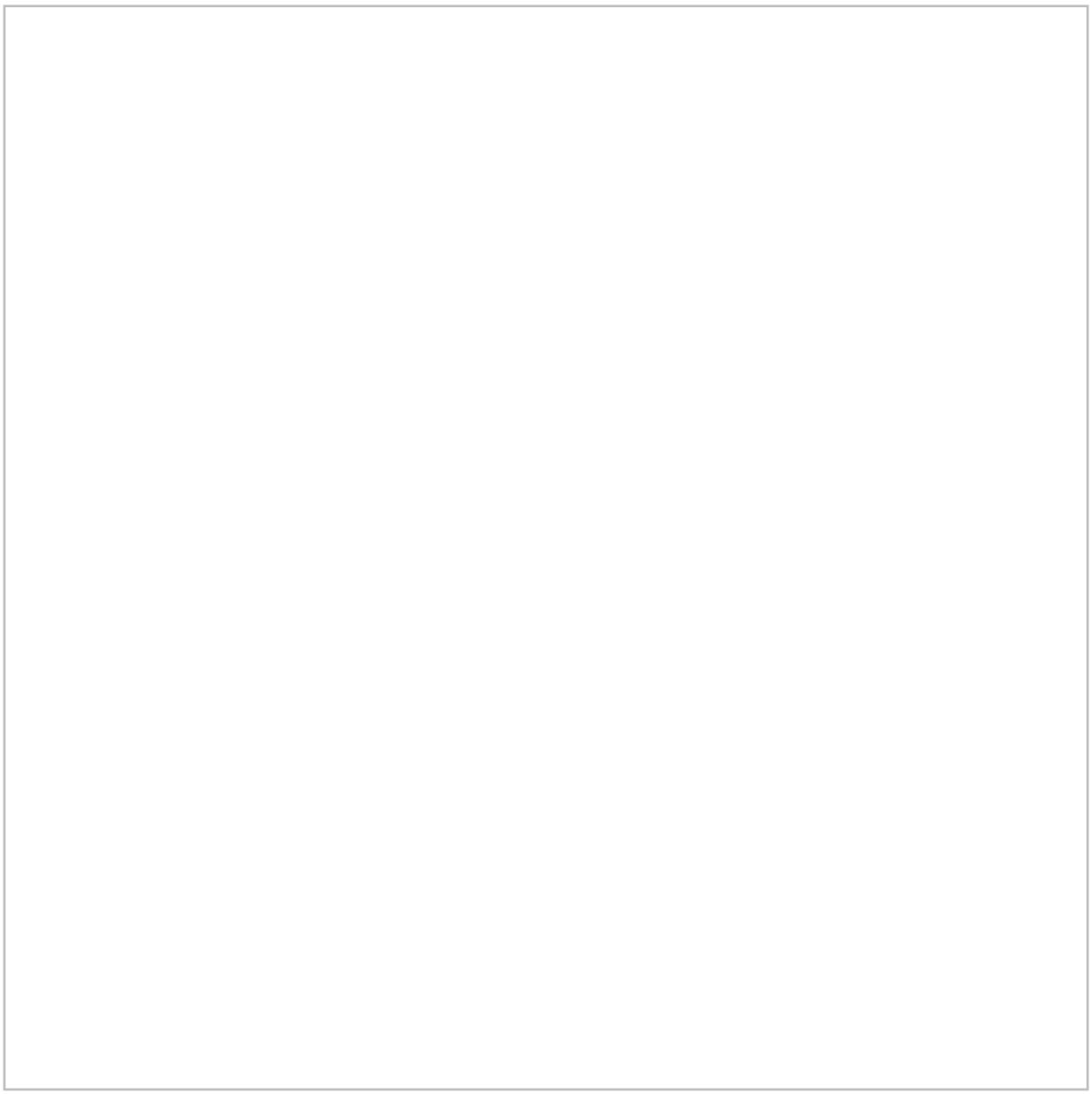
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Richard, Daniel (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:03:55 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.





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

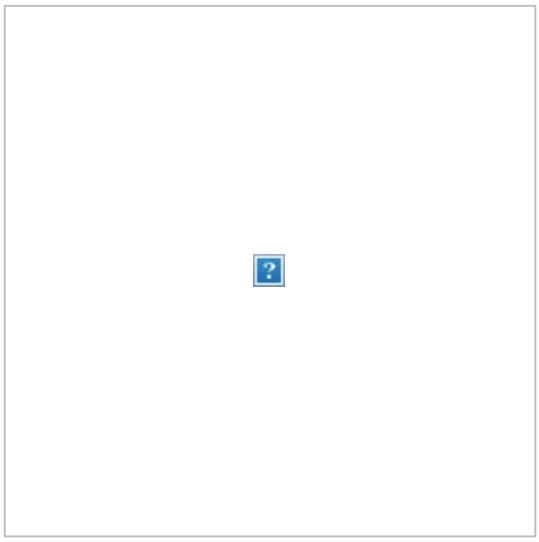
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Burke, Jeffrey (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:03:42 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.



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

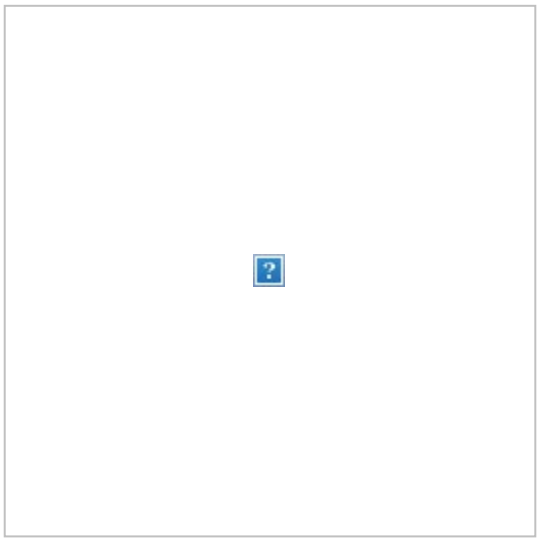
For more information on FINDER visit their website or contact them today!.

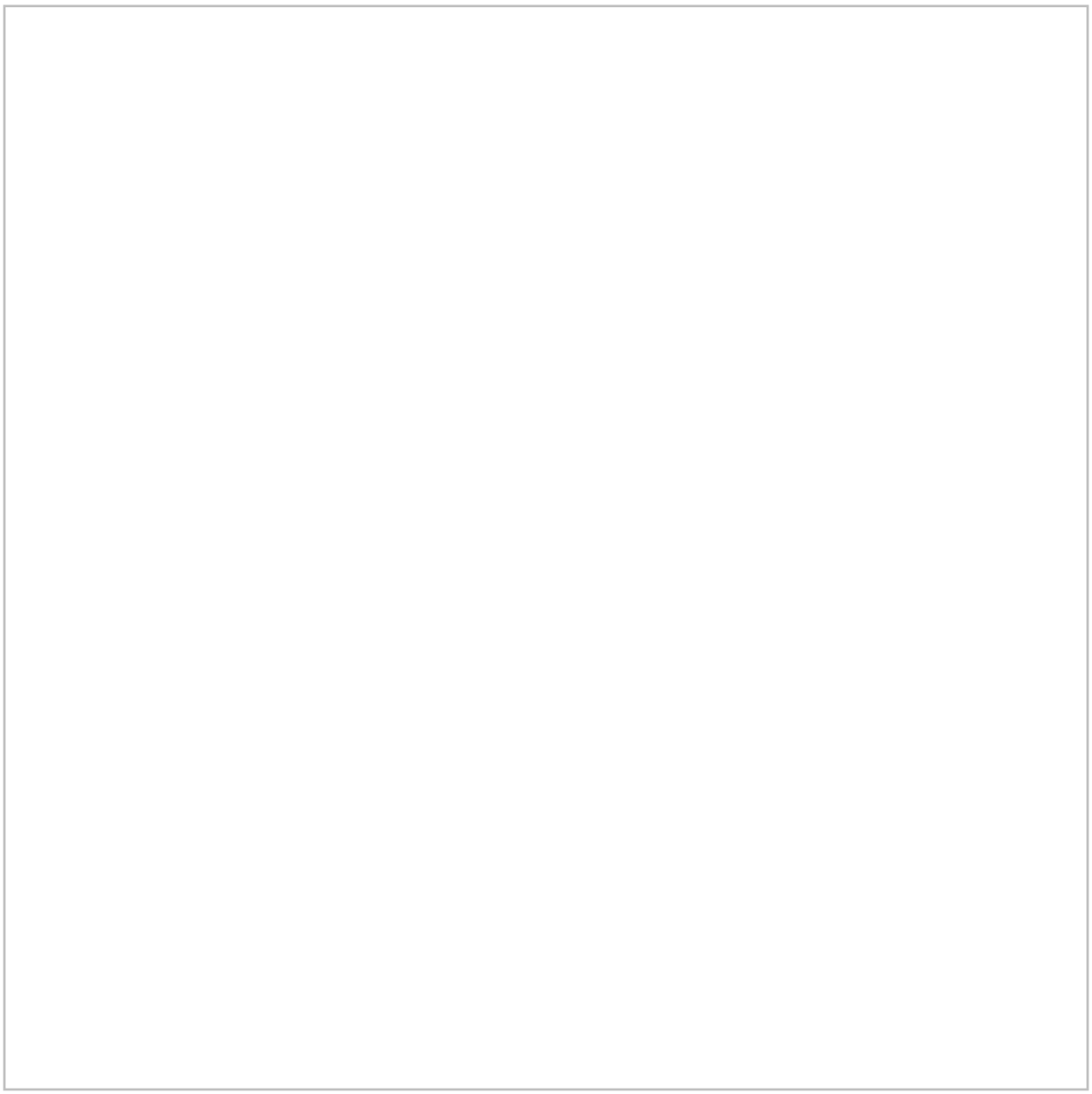
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Bellao, Shaun (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:03:20 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.





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

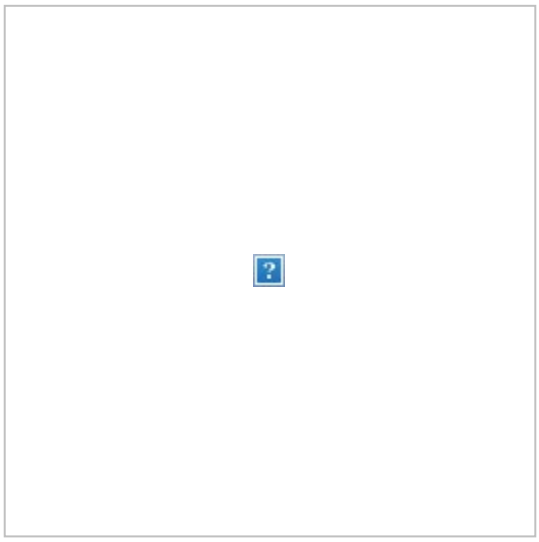
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: McDonald, Steven (EAS)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:03:19 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.



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

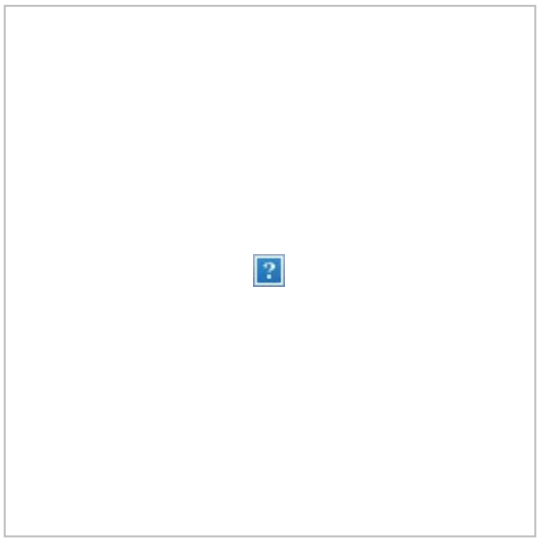
For more information on FINDER visit their website or contact them today!.

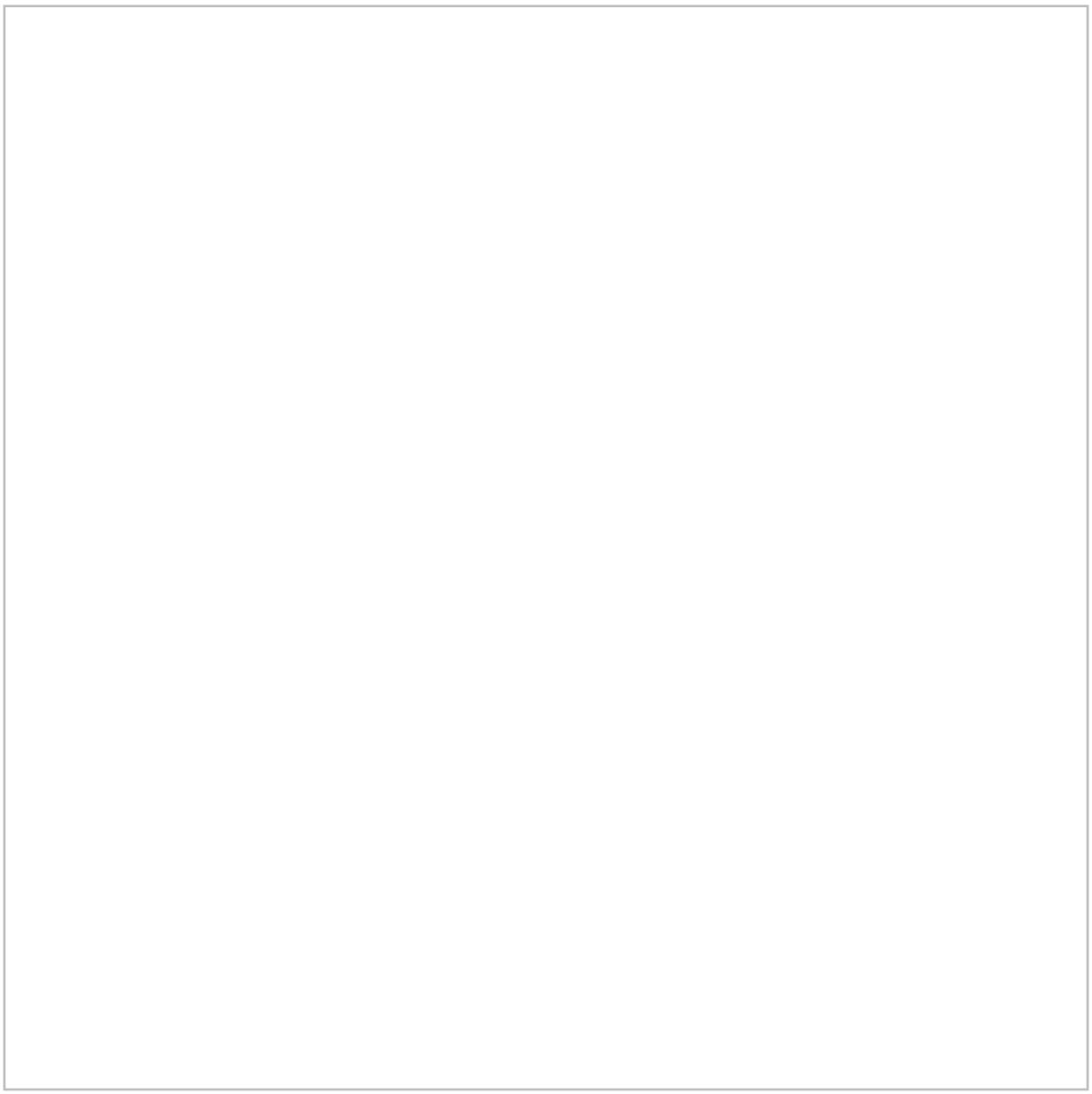
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Collett, David (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:03:19 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.





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

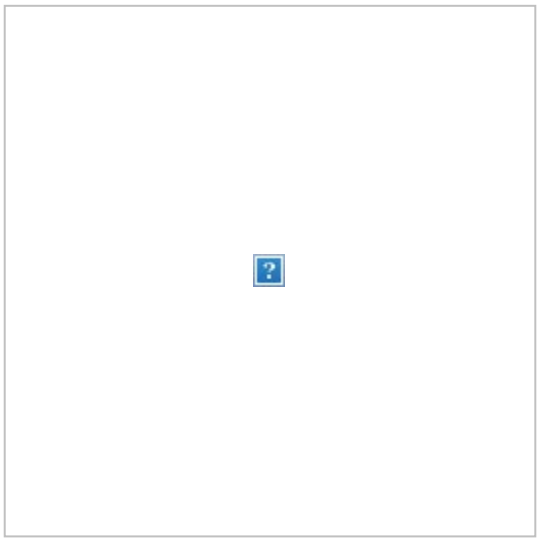
For more information on FINDER visit their website or contact them today!.

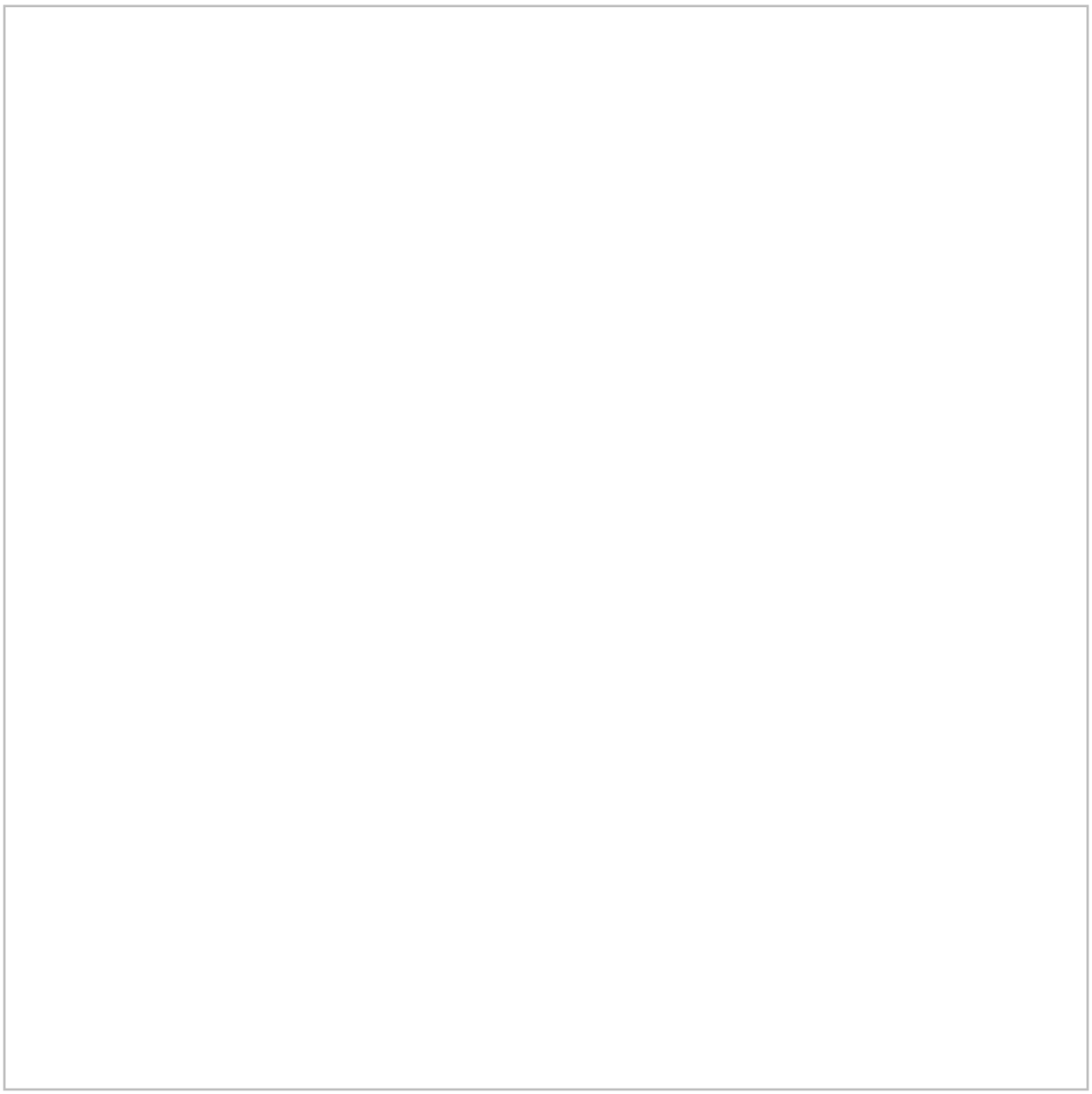
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Wilson, Matthew (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:03:18 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.





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

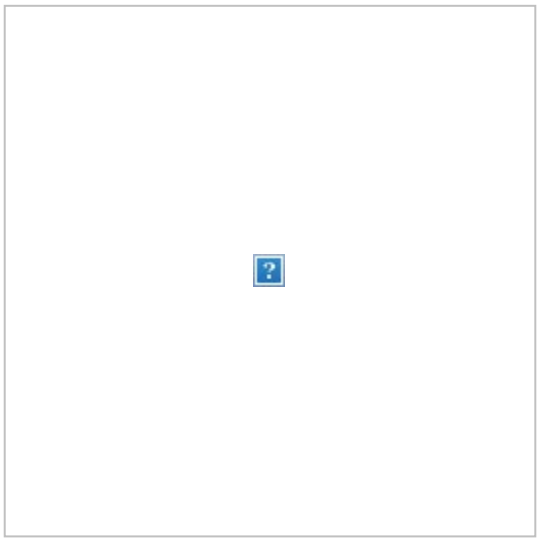
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Sullivan, Thomas W (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 12:03:16 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.



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

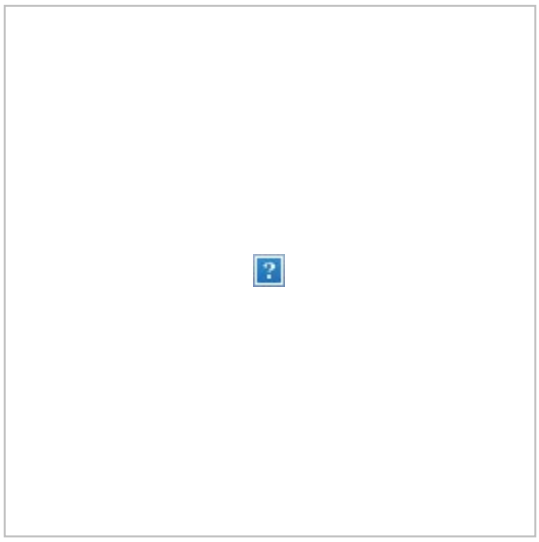
For more information on FINDER visit their website or contact them today!.

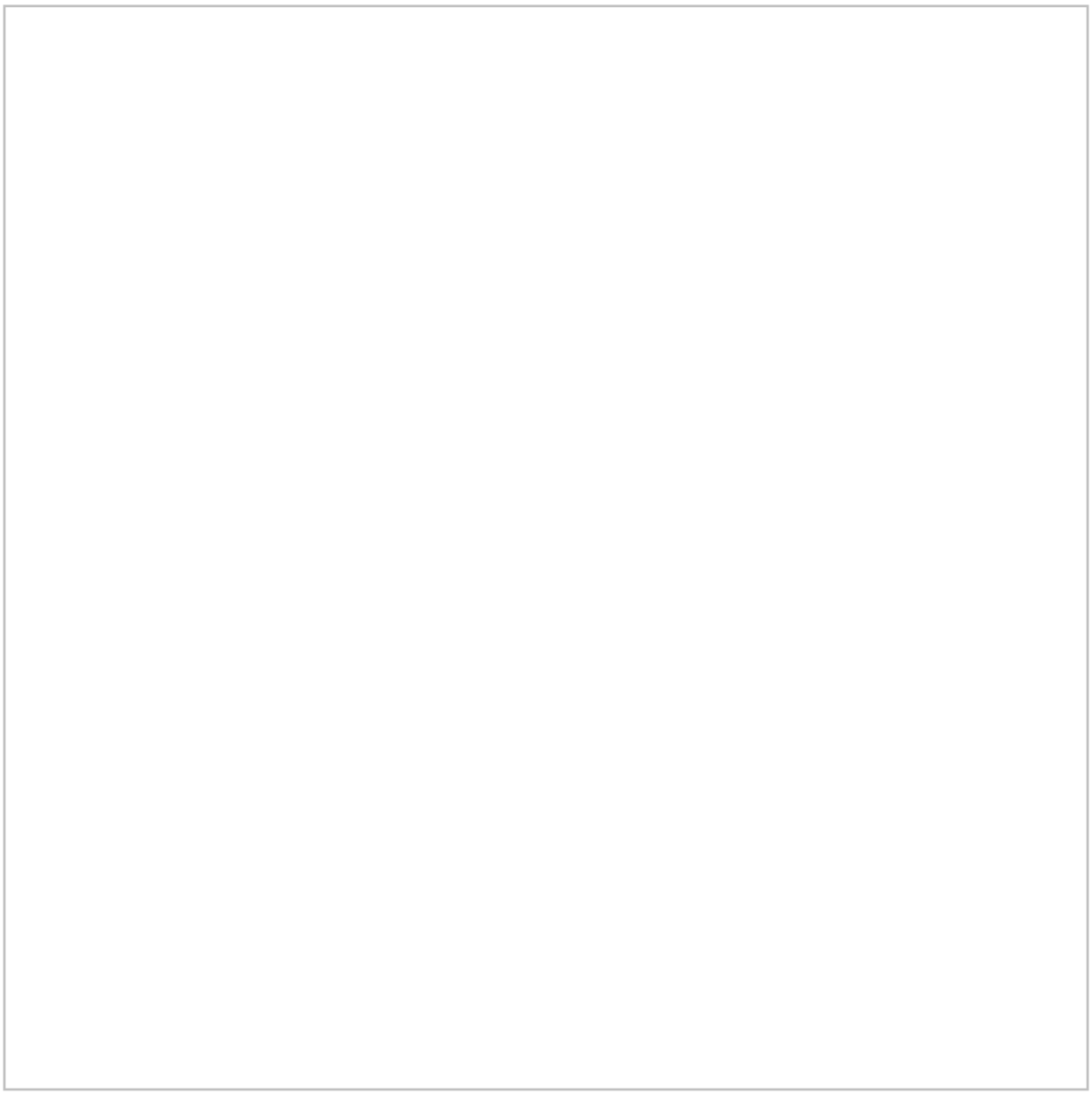
This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Brightman, Scott A (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 11:58:29 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.





Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

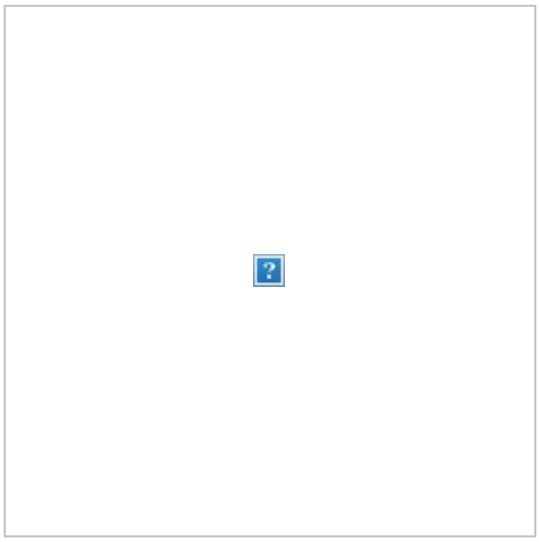
For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: International Homicide Investigators Association
To: Collins, sidney (POL)
Subject: Free Webinar for IHIA Members - FINDER Software Solutions
Date: Tuesday, June 13, 2023 1:07:53 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.



Our Friends at Vetted Security Solutions are offering a free webinar to members of the IHIA. They are a great supporter in providing professional and relevant products to support our mission.

FREE WEBINAR: NO TIME FOR DOWNTIME

Monitor the Health of IP Connected Devices and Minimize Downtime with FINDER Virtual Technician

DATE/TIME: Thursday, June 15, 2023 - 2:00pm EST

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to timely data that can be imperative in your investigations. FINDER Virtual Technician (FVT) is a web-based application that allows system administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have fixed or trailer-mounted systems, FVT monitors all the key hardware and software components of your security intelligence portfolio.

FINDER Software Solutions invites you to join them for a free webinar. We will discuss the following:

• Overview of real-life incidents. What could the outcome have been if they had FVT?

• Live demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

REGISTER TODAY

For more information on FINDER visit their website or contact them today!.

This message was sent to you by International Homicide Investigators Association.
If you no longer wish to receive these emails, you can unsubscribe at any time

https://ihia.org/

From: PoliceGrantsHelp Alert
To: Tulipano, Michael (POL)
Subject: Fund Your License Plate Readers with Grant Money
Date: Tuesday, September 12, 2023 7:00:23 AM

View as webpage | Too many emails? Update Subscription Preferences

ELSAG Radar Trailes



Find Grant Money to Pay for ELSAG® Automatic License Plate Reader Technology



We have partnered with PoliceGrantsHelp.com to help you access government grant dollars

ELSAG Plate Hunter ALPR systems bring incredible efficiencies to real-time policing, security and investigations. Our solutions include fixed, mobile, solar-powered, video-camera and custom plate readers. Each is purpose-built to provide maximum performance for the lowest investment to effectively aid your law enforcement missions. These force-multiplying systems are ideal for:

- Recovering stolen vehicles and license plates
- Removing unregistered vehicles and unlicensed drivers from roads
- Finding missing persons
- Finding vehicles suspected of involvement in unlawful activity
- Parking management and enforcement
- Collecting criminal intelligence
- Permit validation and tolling
- Collection of traffic data

Footer - Email and website. leonardocompany-us.com/lmr



There’s no better time than now to deploy ELSAG automatic license plate readers.

Button - Get Details



Footer - Email and website. leonardocompany-us.com/lmr



Footer - Email and website. leonardocompany-us.com/lmr



If you do not wish to receive future PoliceGrantsHelp Product Alerts, please unsubscribe.
To change your email address, update your profile. © : PoliceGrantsHelp.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: PoliceGrantsHelp Alert
To: Heath, Brendan (POL)
Subject: Fund Your License Plate Readers with Grant Money
Date: Tuesday, September 12, 2023 7:02:11 AM

View as webpage | Too many emails? Update Subscription Preferences

ELSAG Radar Trailes

Find Grant Money to Pay for ELSAG® Automatic License Plate Reader Technology

We have partnered with PoliceGrantsHelp.com to help you access government grant dollars

ELSAG Plate Hunter ALPR systems bring incredible efficiencies to real-time policing, security and investigations. Our solutions include fixed, mobile, solar-powered, video-camera and custom plate readers. Each is purpose-built to provide maximum performance for the lowest investment to effectively aid your law enforcement missions. These force-multiplying systems are ideal for:

- Recovering stolen vehicles and license plates
- Removing unregistered vehicles and unlicensed drivers from roads
- Finding missing persons
- Finding vehicles suspected of involvement in unlawful activity
- Parking management and enforcement
- Collecting criminal intelligence
- Permit validation and tolling
- Collection of traffic data

Footer - Email and website. leonardocompany-us.com/lmr



There’s no better time than now to deploy ELSAG automatic license plate readers.

Button - Get Details



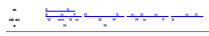
Footer - Email and website. leonardocompany-us.com/lmr



Footer - Email and website. leonardocompany-us.com/lmr



If you do not wish to receive future PoliceGrantsHelp Product Alerts, please unsubscribe.
To change your email address, update your profile. © : PoliceGrantsHelp.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034



om G ant Ma gue t e (N K) <Ma gue te G an @MassMail Sta e MA US>
Sent Monday June 29 2020 3:26 M
To bulkin @wcm ma gov <jbulkant@wcm-ma.gov> mdubo s@fa s ant exema gov <mdubois@fa sant exema gov> mmo gan@b ookl nsema gov <mmo gan@b ookl nsema gov> Be kowi z Kenne h <bke kowit @town canton ma us> mdelu ca@cohasse pol ce com <mde uca@cohassetpo lice com> emon G ego y <gv emmon@cohasse po lice com> Quig ley W l am <wquigley@cohasse po l e com> d Ent emont M chael <mdent emont@pol ce dedham ma gov> McGowan e e <pamcgowan@dove mapol ome> G ace Michael <mg race@ osbo oughpo lice com> Thomas i ynch Rynch@ ank inpol ice com> <t ynch@ ank inpo ice com> m t@ ank inpo ice com <m t@ ank inpol ice com> wam ith@bulk oolpol ice com <wamit h@bu k oolpol ice com> mgue e te@med eld net <mgue e te@med eld net> amting ey@medwaypo ce com <amting ey@medwaypo ce com> coi aye @m l n k net <coi aye @m l n k net > kiag@mpdm ton e g <kiag@mpdm ton e g> j ch l n @tewdhamma gov <jch l ite @tewdhamma gov> cstone@no ok ma us <cstone@no o k ma us> B ooks W l am G. ll <wb ook @no woodma gov> pike ly@no woodma gov <pike ly@no woodma gov> lames Al ed jal ed@pol ce p ainv l e ma us> <jal ed@pol ce p ainv l e ma us> Keenan au <pkeenan@fa quinc ma gov> w l lampa e@ andolphmapol ce com <w l lampa e@ andolphmapol ce com> j o d@ owno sha on o g <j o d@ owno sha on o g> dmcnama a@stoughton ma gov <dmcnama a@stoughton-ma gov> ca michae @wa polepol com> <jca michae @wa polepol com> pi eicki <pj icki @we le lexma gov> kva@wenhampol e g <pj kva@wenhampol e g> G imes Richa d C <g imes@weymouth ma us> <the @jpo ice wenham ma us> richa @jpo ice wenham ma us> Bake Ch s Ell <ch s ba e @mass gov> powe ww2@ e t edu <powe ww2@ e t edu> cromo ly@ u ck k edu <j cromo ly@ u ck k edu> cj omo ly@ou ollk edu> zMcFarlaney Stephen j O] <zcf s ephen zMcfa lane@pol ce ma us> Matthew Rea don m ea don@medwaypol ice com> <m ea don@medwaypol ice com> sakingsbu y@mmedwaypo ice com <wk ingsbu y@mmedwaypol ice com> Hannon John <hannon@ osbo oughpol ice com> B ewe Don <DB ewe @towno sha on s g> Gue ie o M chael (O) <m chael gue ie o@pol tate ma us> Adams ie y p6334@] adams@jpo ice nantucket-ma gov] <jadams@jpo ice nantucket ma gov> Donoghue W l iam NOR] <W l am J Donoghue@MassMa l State MA US> Hun e Avin M63] <Alan Hunte@MassMa l State MA US> on es Steven M [MGC] <steven m on es@MassMail Sta e MA US> Robe t Conno [conno @fbc edu] <conno @fbc edu> Sta rpin Ki Ch ds ptie < sta rpin ki@pp dne ma gov > Sa imini Rama d [O] < sma d ra m m@pol i ate ma us> wwest@mpdm ton e g <wwes @mpdm t on o g> ljabon@b a nt exema gov <ljabon@b a nt exema gov> Gau ding M ichael L <Gau ding.M@westtownsas o g> Kennedy Kev n <dkennedy@ tricon own o g> zzG le David[O] < zDa id zG le@pol ice e ma us> David[lphe ty] ahe dle@fbc edu> <lahe dle@fbc edu> Ma a y Dan <dan el ma a ty.k@fbc edu> Sul liv @gma l com> < Sul liv @gma l com> Antoine Rome e [O] < ome e antoine@pol i ate ma us> Rudolph ames [O] <ames Rudolph@pol ice e ma us> mcol ins@mpdm ton o g <mcol ins@mpdm ton o g> Bu man aul [NOR] < aul Bulman@MassMa l State MA US> antaze os Keith (N K) <keith pan azeliss@MassMa l State MA US> a oli Ma k (N K) <dMa k R a o@MassMa l State MA US> Sul ivan B an [O] <B an Sul van@pol state ma u > yn h Dennis (N K) <Denn s M ynch@Ma sMa l State MA US> owe s Meaghan (N K) <meagh powe s@Ma sMail S ate MA US> D oc o Dav d M [O] <Dav d M Doc co@pol state ma us> Bukhen k Ya ly[O] <ya y bukhenk@pol s ate ma us> Dunne Matthew [O] <Matt hew Dunne@pol state ma u > N chol Kevin [O] <kevin nichol@pol tate ma us> Mat hew Mu phy (mmu phy@b ock onpo ice com) <mmu phy@b ock onpo ice com> ebe lgBs o ktonpo ce com <ebe lgBs ock onpo ice com> a el lg@ho lpo ice g ca el lg@hol pol i e o g> Donovan Ge a d [O] <ge a d donovan@pol tate ma us> b ady@ma b ehead e g <b ady@ma bshead o g> ma thieu ke sch@pl gov <ma thieu ke sch@pl gov> pmclaugh ng@wellesleyma gov <pmc aughl ng@we lles eyma gov> joan ressene@pol boston gov <joan ressene@pol boston gov> Do adose ete <dle ect ves@pow chpo ice o g> ank Noah [O] <noah pack@pol state ma us> Di ll ean Sean (NOR) <Sean Di ll ean@MassMa l State MA US> De aney Ma k (NOR) <ma k delaney@MassMa l State MA US> John e cha d <joe cha d@pe cha d@wenhamo h ma us> O Ne l Reas <one l@fb ook inema gov> hannon Ducha ma@h ospeopo ice com> Del t Mel ssa G eene <me issag eene@ andolphmapo ice com> Bishop Kevin <bishop@towno sha on s g> pende s@towno sha on s g <pende s@towno sha on s g> Anthony Ma ag an homynna ag@ andolphmapo ice com> E ik McNeice o ice O ce ake l e ol ce Depa ment <emche ce@fa e l lema o g> ul e @weymouth ma us < ul e @weymouth ma us> **Cc** Mo ney M chael (N K) <Michael M Mo ney@MassMa l State MA US> Dohe ty Dan ye (N K) <Dann e M Dohe ty@MassMail Sta e MA US> anning ohn (N K) <John m ann ng@MassMa l Sta e MA US> Mat al ons Ge a d (N K) <Ge a d Ma ta lons@MassMail Sta e MA US> Qui K Sears [O] <roan qui.k@pol state ma us> Tu y B ian (N K) <B ian Tul y@MassMail Sta e MA US> N K-D -ADA D ol k <d-N K D -ADA-D ol ct <d-N K D -ADA-Appea s <N K-D -ADA-Appea s@Ma sMail S ate MA US> N K-D -ADA- Appea s <N K-D -ADA-Appea s@Ma sMail S ate MA US>
Subject RE Comm v No man ger a SW o E MO data r E MO mposed as TCOR

Chie s – some mo e ol ow-up on the E MO case I sent a coupl e t week T oope Noah ack had a g eat sugges ion about how to seek n o ma ion om E MO n an invest gat on whe e the e s no C o a pec c suspect th ght ghted h s sugge tion in ed be ow Th s case s uat at ng Stay sa e Ma gue t e

Hi Ma gue te

Thanks o you ep y and discuss on on the ma te Today I ead the decis on n g ea e de ail and I m even mo e u t sted than I was be o e They s a t the dec on by aying that the mpos ion o G S in he i st pace was unsuppo ted so they don t need to add e s he l sue o the sea ch (Unl l ecent y that would be he end o it ight?) Then they ho ough y and by the l own wo ds unnecessa ly add e s he sue o the E MO sea ch by po ice I won t comment u the on that aside to sag a spo nt o how they also did that w th McCa hy

Mo e to he point I t sugge to accept that E MO s ex en ia ly gone as an nvest gative tool because he SJC th nks t s hurt at ng to de endants and unpopu a with he jud cia y The di tinc ion be ween TCOR and p oba ions y use s exsonally clea om he deci on and you emai s and i m not u e we can do much w th hat However i th nk hat s ea ch wa ant o E MO in a ca e without a su pect s a st etch " shing exped t on" s what the Sp ng eld DC cle ks wi l nva ab y he l us as hey deny he appl cat on

The S C c tes Moo e n the inal pa ag aph stating "**To a wa ant oo sea ch o be pe m s o b e unde a t 14 he ag t ma e gove nments n e o este must outwe gh the eve of at se on** I th nk a easonable way to ba ance he gove nment s need to identi y a suspect n a iolent c me against the p i acy inte es s o a G S assigned ind vidual would be the o lowing

1) con act E MO and ask (any ignals we e loca ed n the e xa n quest on
2) I no move on
3) I yes go get a sea ch wa ant o den y the owne o the b ace and his e vant t ave

I would g ue that this p ocedu e d amat cally reduces he nt us on on the ind vidual as h s name and ocat on in o mat on s not di closed to he gove nment unt l a sea ch wa ant is obta ned O ice s have me e y gained enough anonymit ed in o mat on o know that some un nown suspect was he e and to ex abl sh C o get the wa ant o den y t hom

You hough s?

Respect ul y

Noah

T oope Noah H Pack
Massachusetts State o ice Detect ve Unit
O ce o the Hampden D st ct Att o ney
1500 Main St eet 18TH oo
Sp ing eld Massachusetts 01115

Chie s
I ve had a couple o que tions about h s case and I wanted o sha e with ou the ques ions and my answe s The case seems o I ust a e the m ndset o some judges that technolog cal advances like E MO end up being an "un al ad an age" o pol ce

QUESTION #1 Th s l ogical dec s on appea s to c eate a sit o ci umstances whe e an unknown suspect s expec at on o p ivacy cannot be known un l a te a sea ch o E MO data is comp eted wh ch puts pol ce n he pos tion o not know ng whethe it was easonab e no t unt l t s too late t s emin scent o he end o MOCA Pin whe e t was suggested that situ e R desc sions may hinge on how much n o mation comes ba k and not what was a tually ea ched o ever n ght o think! end how wou d you expe t a situ e case to p oy out whe e a suspect is not known so t annot be known i he has his new expectat on o p vacy and pol ce would to que y E MO to deve op a spe t o e ample s me ta Ne York a home mus om ocs s with no suspects pol ice contact E MO o que y any dev ces we e in the a ea pol ce ha n that an E MO's addet was n he a ea pol ce a eg ven den y o suspect pol ice attempt o delete mine whethe suspect is wea ing it as TCOR o post con ict on pol ce a egiven suspect s E MO local on h sto y pol ice inves igate this new suspect At what po nt would a sea h was ant l ikely be equi ed?

Add t onal y do you h nk he e s an avenue o bene t o p otat on o change he TCOR o m and p ocedu e to speci ica ly work n a suspect v ou an a y com en ?

ANSWER #1 Don t e en get me ta ted The Nc mon case came down on Ma ch 17 the l st day o the COVID lockdown and the l ony s that that was ght when the SJC was sta ing to ell udges to let mo e Ds out o ja l on G S b acents So we e going to et all o these peop e out on E MO but hen pol ce can t ea ch he E MO da a? And Dis wi l be out on E MO on even mo e ser ous vio ent c imes n mu t ple cases?

I don t th nk t would he p o p oba ion o change he G S consent o m What the SJC doesn t ell you is _____ t hat he o m s s "**Cou dina es and othe data elated to you phys cal loca ion whi e on GPS a e eco ded and may be sha ed w th the cou t- pbat on pa o e etto neys and law en o ement Data gene a ed by GPS equipment ass gned to you is not p ivate and con dent al**." And in _____ D was ep evented by coun el when he signed it – how mu h mo e volunta y could t be?

The S C s p ob em was that t d not think the e was va id reason o G S The SJC po nted out (at n 2) hat he BMC a g ement had happened mo e han 4 ea s be o e and the t ansc ipt o it was no onge a ai able S noe t s he Commonwealth s bu den to p ove D consen ed to G S the SJC he d hat wi hout the t ansc ipt the Comm cou dn t p ove it – D might ve signed the consent o m ust to get out on bail That seems like a st etch to me- whe e D was ep e en ed by counsel And it s annoy ng to ead hat n 4 that says "the e a e some ins ance" whe e a D might consent to G S but we e not going to ell you what they a e Just like he A R in MCCA Pin I am hope ul hat n anothe s tuation we ll the a g ement t ansc ipt he Commonwealth wou d be able e op ove that D did cons ent o G S -- om what I ve seen de ense a to neys beg judges to put Ds on G S a he than impo e s hghe ba l e pe la ly becau e D don t want to go to al becau e o COVID But pol ice a en t going to know a l that when look ng o the E MO data

We had a t ual on e en ly whe e pol ice deve oped C hat a suspect was inves ed n a e ious c me On he suspect s BO we e open cases in seve al D s e ent ou s wh h the atte mis ion " TCOR " At some ca l ed p obat on and hey sa d he suspect is on E MO and they d we h m the da a without a SW But be au e o like ness he got s W So I wanted to send this ema l a ound o see n pol ce about the is ue

In gene a l would say that when pol ce deve op C hat a spec ic suspect was at the scene o the c me and they have reason to be leve that the suspect was on E MO as a TCOR pol ce should get a SW to ea ch E MO o the u pe t s data You e ight that the tough s tuat on s when pol ice don t ha e a suspect Maybe n a si uation l ke a home invasion o a d ug deal e s house pol ice could w te a SW a idav t o E MO da a n the vic m s yo the c me Th s would be k nd o l ke a geo-enc ng SW which au ho i ea sea ch o cell ne ocat on n o mat on o a phones that fol o w ll ocate t me and the spec ic long/lude/ a t tude o the c me scene) It could say something like "based on in o mat on hat he/she/it/they have reason we e inves ed in d ug dea ing he e's C hat one o mo e pe sons n he a ea we e wea ng E MO/S acke s Based on my t aining and expe ence I know that ou to have ac essing been wea ing de endan s on p e at u ncomfo tmo e wave E MO n cluding in d ug- e ated/ mes ea e o t o the COVID-19 pandemic " That is a t etch but i po ice have no o he eads might be wo th a t y

QUESTION #2 About the case you sent about Elmo in o mat on I neve ask about a pe i ce son even i I have one in mind As a ma te o act I had a B E a ew yea s ago and I u t gave them t me and loca ion I got a ht and t was not he guy I expec ed My equests always say we e the a ny obat one s n he al ini y o such locat on a ound this t me? Does hat round l ke I would wo k? Sounds l ke enough o maybe t the e answe s a pico then get wo ant? I have to guys o wee not to ask o spec i pe son No need and t I m to you

ANSWER #2 A to th s c e i the suspect s BO. say," TCOR "i s best to get a SW o the E MO data I hea you hat it should be bette o police o be open-minded and not spec y u u pe t I suppose you could inc ude in the SW a da it the C you have o suspect #1 and then ask o "data evidenc ng the p evence o su pect #1 o any othe p oba lone wea ng an E MO dev ce n the vic ni y o OCAT ON ON DATE at TIME." That way i the E MO da a comes back that it was someone othe than you suspect you got hat data ju suant to he SW – and data show ng hat suspec #2 was he e wou d be evidence relevant to suspect #1 I t p oves u pe #1 d d n t do t

Thanks o he quest ons – they he p me gu e out how much de ail to put n my ema l s Have a good weekend - Ma gue te



Chie s

In this case he SJC ruled that elect onic moni o ing (E MO) data p ac ng D at the scene o a home nva ion was p ope ly supp essed because D did not consent to E MO as a p et ial cond t on o elease even though D signed a o m ag eeing to t I you a eseeking E MO da a com p obation and E MO was mposed as a p et a cond t on o elea e get a SW

In July 2015 D was a signed n he BMC o pos session o Cass B and moto veh c e v olat ons As p et al cond t ons o release (shown on a Mass c im nal reco d as "**PTCOR**") he was o de ed o stay out o Bos on and wea E MO D signed a o m that said "I have ead and unde stood he above cond t ions and I **ag ee to obse ve them**." A month la e a home invas on and mu dered a med cal e xa min er. D was ep evented by coun el when he signed it – how mu h mo e volunta y could t be? The S C s p ob em was that t d not think the e was va id reason o G S The SJC po nted out (at n 2) hat he BMC a g ement had happened mo e han 4 ea s be o e and the t ansc ipt o it was no onge a ai able S noe t s he Commonwealth s bu den to p ove D consen ed to G S the SJC he d hat wi hout the t ansc ipt the Comm cou dn t p ove it – D might ve signed the consent o m ust to get out on bail That seems like a st etch to me- whe e D was ep e en ed by counsel And it s annoy ng to ead hat n 4 that says "the e a e some ins ance" whe e a D might consent to G S but we e not going to ell you what they a e Just like he A R in MCCA Pin I am hope ul hat n anothe s tuation we ll the a g ement t ansc ipt he Commonwealth wou d be able e op ove that D did cons ent o G S -- om what I ve seen de ense a to neys beg judges to put Dson G S a he than impo e s hghe ba l e pe la ly becau e D don t want to go to al becau e o COVID But pol ice a en t going to know a l that when look ng o the E MO data

We had a t ual on e en ly whe e pol ice deve oped C hat a suspect was inves ed n a e ious c me On he suspect s BO we e open cases in seve al D s e ent ou s wh h the atte mis ion " TCOR " At some ca l ed p obat on and hey sa d he suspect is on E MO and they d we h m the da a without a SW But be au e o like ness he got s W So I wanted to send this ema l a ound o see n pol ice about the is ue

In gene a l would say that when pol ice deve op C hat a spec ic suspect was at the scene o the c me and they have reason to be leve that the suspect was on E MO as a TCOR pol ice should get a SW to ea ch E MO o the u pe t s data You e ight that the tough s tuat on s when pol ice don t ha e a suspect Maybe n a si uation l ke a home invasion o a d ug dea e s house pol ice could w te a SW a idav t o E MO da a n the vic ni y o the c me Th s would be k nd o l ke a geo-enc ng SW which au ho i ea sea ch o cell ne ocat on n o mat on o a phones that fol o w ll ocate t me and the spec ic long/lude/ a t tude o the c me scene) It could say something like "based on in o mat on hat he/she/it/they have reason we e inves ed in d ug dea ing he e's C hat one o mo e pe sons n he a ea we e wea ng E MO/S acke s Based on my t aining and expe ence I know that ou to have ac essing been wea ing de endan s on p e at u ncomfo tmo e wave E MO n cluding in d ug- e ated/ mes ea e o t o the COVID-19 pandemic " That is a t etch but i po ice have no o he eads might be wo th a t y

Ju suant to he SW – and data show ng hat suspec #2 was he e wou d be evidence relevant to suspect #1 I t p oves u pe #1 d d n t do t

Thanks o he quest ons – they he p me gu e out how much de ail to put n my ema l s Have a good weekend - Ma gue te

M r a. d e T. Gr ue
G a r J C ins t - Distr c tTE ining
O ffice (N e B Dr. ive A v enue Mich I W. M ssa ey
65 h ventBo d
C a b, MA 02903
781- 30-8839

From: Thibault, Amy (POL)
To: Smith, Eleanor (POL)
Subject: FW: HSOC LPR Training 9/14/2023
Date: Wednesday, September 6, 2023 10:15:00 AM

Hi Elly,
I saw you weren't on here. Do you know if we're getting access to LEARN?
It looks like there is training below (I wonder if they can get them to stay past 3pm) and everyone will have to refresh themselves of TRF-11, especially the section below on Non-departmental ALPR Systems.

Use of Non-Departmental ALPR Systems
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.
Supervisors and analysts assigned to the Commonwealth Watch Center/Commonwealth Fusion Center and the ALPR Administrator may access non-departmental ALPR systems for official law enforcement purposes as authorized by this policy. 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, retention, and quality assurance standards than the Department's ALPR system. Members shall be mindful to preserve, export, or obtain copies of records or reports that are of known relevance to an incident or investigation prior to the expiry of the records.

From: Walczak, Ryan (POL) <ryan.walczak@pol.state.ma.us>
Sent: Tuesday, September 5, 2023 2:17 PM
To: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Cc: Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Rudolph, James (POL) <James.Rudolph@pol.state.ma.us>; Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>
Subject: Fw: HSOC LPR Training 9/14/2023

Good Afternoon,

We are meeting with Motorola on 9/14/2023 @0900HRS to approximately 1500HRS at GHQ HSOC. This will be a training given by Motorola in regards to the ALPR System "LEARN". Moving forward, this training will be mandatory for access to the system. There is currently no tentative date for a second training at this time. We strongly recommend that anyone in your unit who has access to, or uses the ALPR system in their current job title attend this training.

Respectfully,
Ryan

Sergeant Ryan Walczak #3731
Massachusetts State Police
Division Of Homeland Security and Preparedness
Technical Services Unit
G.L. c. 4.sec. 7.cl.26 (n)(security)
Email: Ryan.walczak@pol.state.ma.us

From: Walczak, Ryan (POL)
Sent: Tuesday, September 5, 2023 1:20 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Accepted: HSOC LPR Training
When: Thursday, September 14, 2023 9:00 AM-4:00 PM.
Where: 470 Worcester Road, Framingham, MA

From: Pack, Noah (POL)
To: Cyr, Mark (POL)
Subject: Fw: Language Draft
Date: Thursday, March 2, 2023 11:11:22 AM

The Massachusetts Supreme Judicial Court has recognized that individuals have a reasonable expectation of privacy in the whole of their public movements (see *Commonwealth vs. McCarthy, 484 Mass. 493*). While the SJC indicated that the limited use of ALPR does not infringe upon a constitutional right, and therefore does not require legal process, the widespread or long-term use of ALPR may be sufficiently detailed to invade a reasonable expectation of privacy. Members should in active criminal investigations that do not involve exigent circumstances should be reviewed with a prosecutor of jurisdiction in the investigation for review of the potential necessity of a search warrant.

Sir, this is what I had in a draft (it is in the one I sent a few weeks ago) but was not in the one I sent them yesterday:

The Massachusetts Supreme Judicial Court has recognized that individuals have a reasonable expectation of privacy in the whole of their public movements (see *Commonwealth vs. McCarthy, 484 Mass. 493*). While the SJC indicated that the limited use of ALPR does not infringe upon a constitutional right, and therefore does not require a search warrant or other legal process, the widespread and long-term use of ALPR to investigate an individual may amount to a constitutional violation.

Combining this with their suggestions, it could look like:

The Massachusetts Supreme Judicial Court has recognized that individuals have a reasonable expectation of privacy in the whole of their public movements (see *Commonwealth vs. McCarthy, 484 Mass. 493*). While the SJC indicated that the limited use of ALPR does not infringe upon a constitutional right, and therefore does not require legal process, the extensive or long-term use of ALPR in active criminal investigations that do not involve exigent circumstances should be reviewed with a prosecutor of jurisdiction in the investigation for review of the potential necessity of a search warrant.

I'll review McCarthy again for other thoughts.

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: Cyr, Mark (POL)
To: Pack, Noah (POL)
Subject: Fw: MSP Request for Flock Subscription
Date: Friday, November 17, 2023 2:54:26 PM

Lieutenant Colonel Mark D. Cyr #2728
Massachusetts State Police
Division Commander
Division of Homeland Security and Preparedness
508-988-7301 (office)
G.L. c. 4.sec. 7.cl.26 (n)(security)

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: Kwon, Gina K. (EPS) <Gina.K.Kwon@mass.gov>
Sent: Friday, November 17, 2023 1:59 PM
To: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Subject: FW: MSP Request for Flock Subscription

Suggested that MSP be part of this briefing. Should be you or someone else? Let me know…and we can schedule.

Gina K. Kwon
Undersecretary for Law Enforcement
Mobile: G.L. c. 4.sec. 7.cl.26 (n)(security)

From: Kesselheim, Dara Z. (GOV) <Dara.Z.Kesselheim@mass.gov>
Sent: Friday, November 17, 2023 12:18 PM
To: Kwon, Gina K. (EPS) <Gina.K.Kwon@mass.gov>; Boodoo, Jesse M. (GOV) <Jesse.M.Boodoo@mass.gov>; Melander, John (EPS) <John.Melander@mass.gov>; Baldwin, Cecilia Ugarte (GOV) <Cecilia.Baldwin@mass.gov>; Rebello-Pradas, Alicia (GOV) <Alicia.M.Rebello-Pradas@mass.gov>
Cc: Walker, Suleyken (EPS) <Suleyken.Walker@mass.gov>
Subject: RE: MSP Request for Flock Subscription

Hi Gina:

I will be running point on the Flock subscription issue for GLO. Can we set up a time for a short briefing on this? Specifically, I'm interested in learning more about MSP's need for/objectives in using Flock, and your analysis with respect to how the use of this type of system would comport with the analysis set forth by the SJC in *Commonwealth v. McCarthy*, 484 Mass. 493, 505-508 (2020). This

will require some explanation as to the capabilities of the cameras used by Flock, the retention for data captured, etc. *See id*. at 508. It would be helpful for our Policy and Leg Affairs people (copied) to be in the room for this briefing so that we can all think collaboratively about this.

Thanks,

DZK

From: Kwon, Gina K. (EPS) <Gina.K.Kwon@mass.gov>
Sent: Wednesday, November 15, 2023 11:15 AM
To: Boodoo, Jesse M. (GOV) <Jesse.M.Boodoo@mass.gov>; Melander, John (EPS) <John.Melander@mass.gov>
Cc: Walker, Suleyken (EPS) <Suleyken.Walker@mass.gov>; Kesselheim, Dara Z. (GOV) <Dara.Z.Kesselheim@mass.gov>
Subject: RE: MSP Request for Flock Subscription

Hi Jesse,

There's no specific timeline for this, but this is also related to a request that MSP/EOPSS made to MassDOT about hanging LPR cameras on MassDOT infrastructure. You may recall that you connected me with MassDOT attorneys over the summer about this. [redacted: G.L. c. 4.sec. 7.cl.26 (n)(security); G.L. c. 4.sec. 7. cl.26(f)(investigative)]
[redacted]
MSP has money, which needs to be spent this FY, that they would like to spend on those LPR cameras if MassDOT allows use of their gantries and structures—they would need to make those orders in the next few months.

In my mind, I see these two issues as related, so I wanted to raise that background. So, no timeline for Flock, but there is one related to the request to MassDOT. I would also note that this is a priority for MSP and I would also echo and support that sentiment at the EOPSS level.

Hope that helps.
Gina

Gina K. Kwon
Undersecretary for Law Enforcement
Mobile: [redacted: G.L. c. 4.sec. 7.cl.26 (n)(security)]

From: Boodoo, Jesse M. (GOV) <Jesse.M.Boodoo@mass.gov>
Sent: Wednesday, November 15, 2023 9:14 AM
To: Melander, John (EPS) <John.Melander@mass.gov>
Cc: Kwon, Gina K. (EPS) <Gina.K.Kwon@mass.gov>; Walker, Suleyken (EPS) <Suleyken.Walker@mass.gov>; Kesselheim, Dara Z. (GOV) <Dara.Z.Kesselheim@mass.gov>
Subject: RE: MSP Request for Flock Subscription

Adding Dara. Is there a timeline for decision on this?

From: Melander, John (EPS) <John.Melander@mass.gov>
Sent: Wednesday, November 15, 2023 7:31 AM
To: Boodoo, Jesse M. (GOV) <Jesse.M.Boodoo@mass.gov>
Cc: Kwon, Gina K. (EPS) <Gina.K.Kwon@mass.gov>; Walker, Suleyken (EPS) <Suleyken.Walker@mass.gov>
Subject: Re: MSP Request for Flock Subscription

Hi Jesse,

Please find the policy attached.

Thank you,
John

From: Boodoo, Jesse M. (GOV) <Jesse.M.Boodoo@mass.gov>
Sent: Tuesday, November 14, 2023 8:07:49 PM
To: Melander, John (EPS) <John.Melander@mass.gov>
Cc: Kwon, Gina K. (EPS) <Gina.K.Kwon@mass.gov>; Walker, Suleyken (EPS) <Suleyken.Walker@mass.gov>
Subject: RE: MSP Request for Flock Subscription

Thanks can you forward the ALPR policy?

From: Melander, John (EPS) <John.Melander@mass.gov>
Sent: Tuesday, November 14, 2023 4:29 PM
To: Boodoo, Jesse M. (GOV) <Jesse.M.Boodoo@mass.gov>
Cc: Kwon, Gina K. (EPS) <Gina.K.Kwon@mass.gov>; Walker, Suleyken (EPS) <Suleyken.Walker@mass.gov>
Subject: MSP Request for Flock Subscription

Good Afternoon Jesse,

Attached for your consideration is a brief memo outlining MSP's request to obtain a subscription to Flock – a company that operates ALPR cameras throughout the state. Gina may have flagged this issue for you, but regardless she asked that I send it up for your (or your team's) review. It might make sense to have a brief meeting after you have a chance to take a look at the memo. We're happy to address any questions or concerns.

Thank you,

John Melander
Deputy General Counsel
Executive Office of Public Safety and Security

One Ashburton Place, Suite 2133
Boston, MA 02108
[redacted] G L. c. 4.sec. 7.cl.26 (n)(security)

From: Bernstein, Eric (POL)
To: Henneberry, Derek (POL)
Subject: FW: Quote for upgrades and repairs
Date: Wednesday, October 4, 2023 9:27:08 AM

Derek,

Please set up a meeting with these guys and figure out where the system currently stands, and what is would costs to get some of the mobile ALPRs back operational. Thank you.

Respectfully,

Lt. Eric S. Bernstein #2308
Commander, Traffic Programs Section
Commander, Public Order Platoon
Massachusetts State Police
774-462-3762 (office)
G L. c. 4 sec. 7.cl.26 (n)(security)
eric.bernstein@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 notify the sender immediately. Thank you.*

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Monday, August 7, 2023 9:06 PM
To: Bernstein, Eric (POL) <eric.bernstein@pol.state.ma.us>
Cc: Walczak, Ryan (POL) <ryan.walczak@pol.state.ma.us>
Subject: Re: Quote for upgrades and repairs

Lt, please see comments in line.

Respectfully,

Sergeant Noah H. Pack
Massachusetts State Police

From: Bernstein, Eric (POL) <eric.bernstein@pol.state.ma.us>
Sent: Monday, August 7, 2023 19:56
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Walczak, Ryan (POL) <ryan.walczak@pol.state.ma.us>
Subject: RE: Quote for upgrades and repairs

Noah,

Thanks for all your efforts to help keep these systems up and running. So you are saying that the 2 brand new systems installed last September are both broken now and not covered under warranty to service them?

The product warranty does not cover service. I believe that we tried to include it, but the grant rules prohibited including the service package with the purchase. These units require a software update and general routine service from a technician, and despite some issues with the hardware in one of them, which was covered under warranty, I believe they can be back in service when that update is completed.

As of last November we had 9 systems operational. Do you have an updated spreadsheet that show the assignment and status of each?

The spreadsheet for the DFS units is up to date as to the general status of the units. Some of the units which were operational last year are older models (SX3s), and these no longer meet the standards to use with the system. There are four systems that meet the standard (SX4s), including the two new ones and two somewhat older ones that were reinstalled last year as hand me downs from CVES. The latter two have experienced failures of various components and require on site service. I believe we have the necessary parts for the repairs.

I also understand that these systems never received license suspension data from the RMV as was required by the grant agreement.

I'm unaware of any grant requirements stipulating this. Nonetheless, it was certainly a goal and we have been working with CJIS to get that set up for the traffic programs units. The new file was built, and CJIS has been working with the vendor to find a way to transfer and upload the file, which so far has not been resolved. This project also took a bit of a backseat since the units are off-line.

Based on all these facts I am extremely hesitant to ask for any additional funds towards these systems. You were looking at another vendor with a more reliable system, what is the status of that?

I would not fault you for that hesitation. These systems has proven complicated and time consuming to keep operational due to various hardware and software challenges. However, it's fair to say that the four units that are serviceable would be effectively abandoned if it were decided not to invest any further in them. In this case, some time could be bought with small money while future options are reviewed, such as a regular service package. These units will never be maintenance cost free as long as we seek to keep them running correctly. We are continuing to explore options, which we can discuss further on the phone if you'd like.

Perhaps we could have a conference call on Wednesday or Thursday to discuss?

We should be available for a call Wednesday between 9 and 10 AM and 12 and 3 PM. If that doesn't work Thursday morning may work as well.

Respectfully,
Lt. Eric S. Bernstein #2308
Commander, Traffic Programs Section
Commander, Public Order Platoon
Massachusetts State Police
774-462-3762 (office)
G L. c. 4 sec. 7.cl.26 (n)(security)
eric.bernstein@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 notify the sender immediately. Thank you.*

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Monday, August 7, 2023 4:16 PM
To: Bernstein, Eric (POL) <eric.bernstein@pol.state.ma.us>
Cc: Walczak, Ryan (POL) <ryan.walczak@pol.state.ma.us>
Subject: Re: Quote for upgrades and repairs

Lt Bernstein,

Following up on the DFS LPRs. First a heads up: Sergeant Ryan Walczak of the Technical Services Unit is now the ALPR Administrator for the Department, and I am currently bringing him up to speed on the various aspects of the program.

Second, there are currently four cruisers in DFS (excluding CVES) which have ALPR systems which should be serviceable going forward. The older processors are no longer useable due to their age and capabilities. As these older cruisers are deadlined, the systems can be removed and will not be reinstalled.

All four of the newer units are currently out of service pending updates/service. Attached is a quote to service them. I also had him update the quote to include installing a system into a cruiser, which should allow us to use other equipment that we currently have available but not in service.

Please advise if you would like to write the request to fund these or if you would like us to.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Tuesday, July 11, 2023 9:06 PM
To: Bernstein, Eric (POL) <eric.bernstein@pol.state.ma.us>
Subject: Fwd: Quote for upgrades and repairs

Lt Bernstein,

Please see the attached quote for repairs and service related to traffic programs' 4 newest cruiser LPRs. All are currently out of service pending updates and repairs.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

From: Kory Koster <kkoster@329marketinginc.com>
Sent: Tuesday, July 11, 2023 8:59:20 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Quote for upgrades and repairs

CAUTION: This email originated from a sender outside of the 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 Sgt,

Attached is the quote for the repairs and upgrades you requested

--
Kory Koster

329 Marketing Inc.
Public Safety Sector
508 989 2783
kkoster@329marketinginc.com

From: LaBelle, Keri (POL)
To: Sarah Roseman
Subject: FW: Request to connect for discussing GeoShield RTCC Solution.
Date: Tuesday, May 30, 2023 8:49:00 AM

Keri L. LaBelle, ABC
Forensic Scientist III – Quality Assurance
Massachusetts State Police
124 Acton Street
Maynard, MA 01754
Direct: 978-451-3317
Email: keri.labelle@pol.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.

All communications sent or received by this Commonwealth of Massachusetts email address may be subject to disclosure under the Massachusetts Public Records Law (M.G.L. Chapter 66, Section 10) and the Federal Freedom of Information Act.

Your feedback is important to us. We value your input to continuously improve and provide you with the best possible service. Please let us know how we are doing by taking our short survey at the following link: MSP Crime Laboratory Service Satisfaction Survey

---

From: Arunima Choudhary <arunima.choudhary@spatialitics.com>
Sent: Thursday, May 25, 2023 10:50 AM
To: LaBelle, Keri (POL) <Keri.LaBelle@pol.state.ma.us>
Subject: Request to connect for discussing GeoShield RTCC Solution.

CAUTION: This email originated from a sender outside of the 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 Keri,

Hope this email finds you well.

I have been attempting to contact you several times in the past especially in my last mail on 2nd May'23 which elaborated our GeoShield RTCC Solution:

1. Uniquely connects multiple data sources like CAD, RMS, AVL, ALPR, etc.
2. Re-Designed Dashboard for Immersive Experience & Quick Access.
3. City Monitoring and Situational Awareness.
4. Advanced Mapping and Spatial Analytics.

My purpose in reaching out to you today is to inquire whether you anticipate a need for the RTCC Solution mentioned above within coming years.

Would like to offer our assistance by providing you a one-on-one interactive session with our experts to give you a better understanding of the potential scope of the Real-Time Crime Center initiatives for 2023-2024.

To facilitate this, would propose scheduling a call at a mutually convenient time.

Look forward to hearing from you soon.

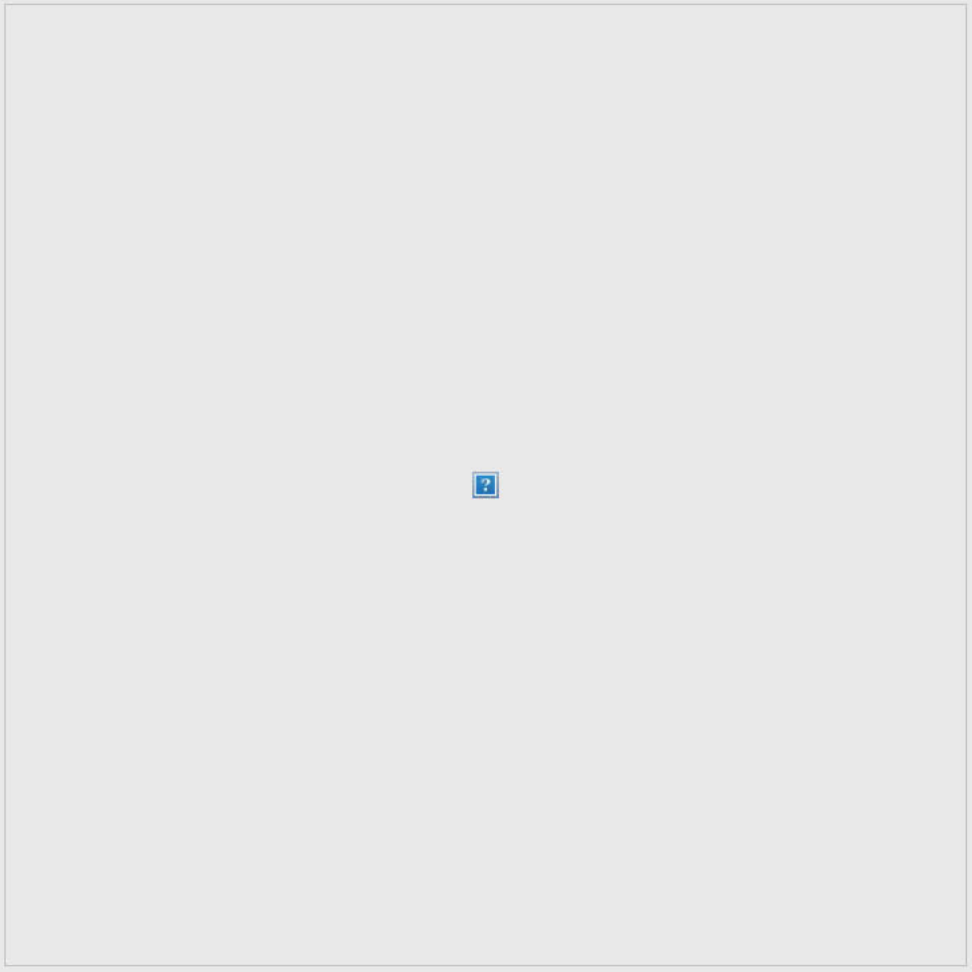
Thank you.

Cheers,
Arunima Choudhary
(630) 214 – 9787
arunima.choudhary@spatialitics.com

From: POLICE
To: McCarthy, Jeffrey (POL)
Subject: Get POLICE"s Top How-To"s
Date: Monday, May 1, 2023 12:33:18 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.

May 01, 2023



FREE WHITEPAPERS



Sponsored by VirTra

What To Look For in Simulation Training

So, you are on the hunt for new training technology to improve the learning, experience and retainment of knowledge for your agency. You'll likely be wondering where to begin and what to look for in a good system. This guide will give you an idea of how t

DOWNLOAD



Sponsored by POLICE, Leonardo & LexisNexis Coplogic

SPECIAL REPORT: Traffic Safety and Enforcement

In this POLICE Special Report: Traffic Safety and Enforcement, read about new technologies in accident prevention and roadway monitoring.

DOWNLOAD



Sponsored by Collective Data

The Tennessee Department of Public Safety Increased Visibility, Accountability and Accuracy with Inventory Management Software Designed Specifically for Law Enforcement

Before implementing new software, TDPS was using spreadsheets alongside an outdated asset management system without flexibility to meet the department's needs resulting in many inefficiencies.

DOWNLOAD



Sponsored by POLICE, Adamson Industries, Traka USA/Assa Abloy

Special Report: Fleet Management Solutions

In this POLICE Special Report: "Fleet Management Solutions" read about some key issues in the maintenance and management of law enforcement vehicles. Learn 15 factors to consider when choosing an upfitter.

DOWNLOAD



Sponsored by POLICE

Special Report: Traffic Safety and Enforcement

Read about how e-citation systems are making traffic stops safer for officers and motorists, how motorists can work with police to report non-injury traffic accidents, how automatic license plate recognition (ALPR) systems can help agencies monitor traffic patterns, and how crash mapping can predict when and where accidents are likely to occur.

DOWNLOAD

POLICE MAGAZINE

You are currently subscribed as jeffrey mccarthy@pol.state.ma.us.

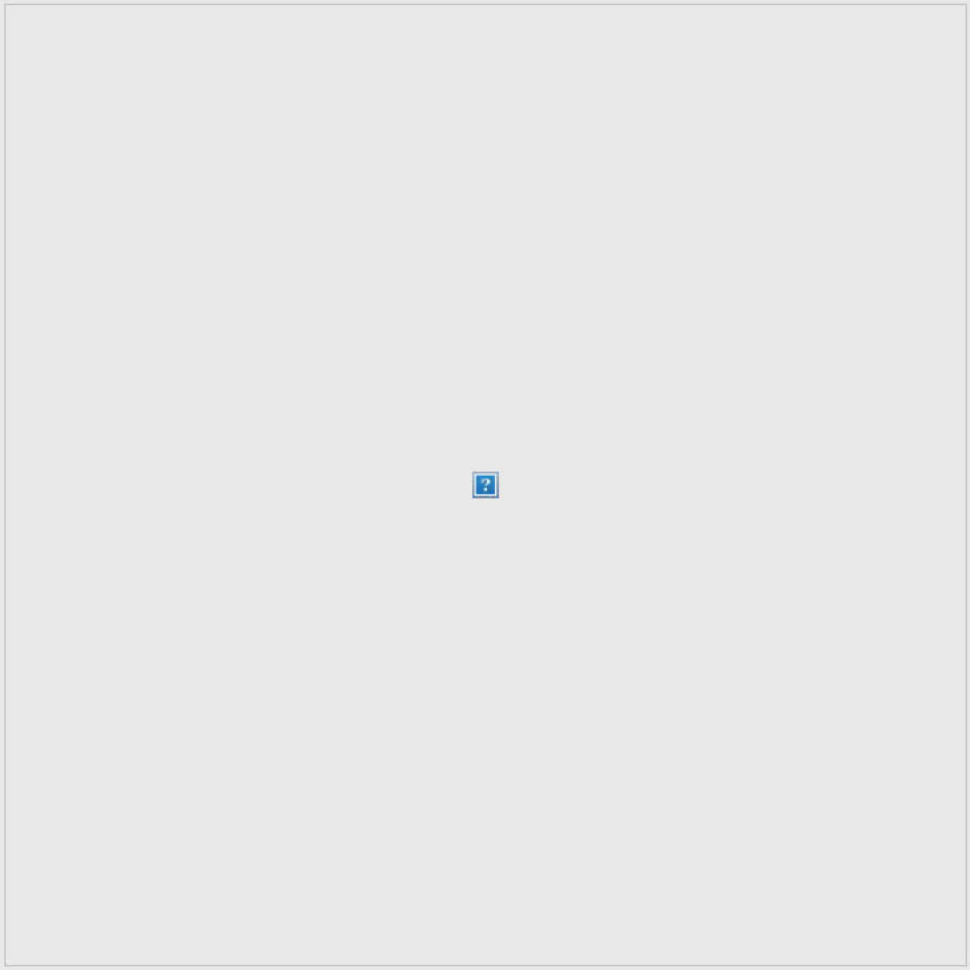
Bobit Business Media is located at 21250 Hawthorne Blvd, Suite 360, Torrance CA 90503

Contact Us | Privacy Policy | Unsubscribe

From: POLICE
To: McCarthy, Jeffrey (POL)
Subject: Get POLICE"s Top How-To"s
Date: Monday, April 17, 2023 12:33:11 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.

Apr 17, 2023



FREE WHITEPAPERS



Sponsored by VirTra

What To Look For in Simulation Training

So, you are on the hunt for new training technology to improve the learning, experience and retainment of knowledge for your agency. You'll likely be wondering where to begin and what to look for in a good system. This guide will give you an idea of how t

DOWNLOAD



Sponsored by POLICE, Leonardo & LexisNexis Coplogic

SPECIAL REPORT: Traffic Safety and Enforcement

In this POLICE Special Report: Traffic Safety and Enforcement, read about new technologies in accident prevention and roadway monitoring.

DOWNLOAD



Sponsored by Vector Solutions

CHECKLIST: Does Your Early Warning System Do These 4 Things?

Many of the early warning systems on the market today offer the same basic functionality for behavior tracking, use of force tracking, and other hot topics. Download this checklist to find out if your system has the right features.

DOWNLOAD



Sponsored by Collective Data

The Tennessee Department of Public Safety Increased Visibility, Accountability and Accuracy with Inventory Management Software Designed Specifically for Law Enforcement

Before implementing new software, TDPS was using spreadsheets alongside an outdated asset management system without flexibility to meet the department's needs resulting in many inefficiencies.

DOWNLOAD



Sponsored by POLICE, Adamson Industries, Traka USA/Assa Abloy

Special Report: Fleet Management Solutions

In this POLICE Special Report: “Fleet Management Solutions” read about some key issues in the maintenance and management of law enforcement vehicles. Learn 15 factors to consider when choosing an upfitter.

DOWNLOAD

Sponsored by POLICE

Special Report: Traffic Safety and Enforcement

Read about how e-citation systems are making traffic stops safer for officers and motorists, how motorists can work with police to report non-injury traffic accidents, how automatic license plate recognition (ALPR) systems can help agencies monitor traffic patterns, and how crash mapping can predict when and where accidents are likely to occur.

DOWNLOAD

POLICE MAGAZINE

You are currently subscribed as jeffrey mccarthy@pol.state.ma.us.

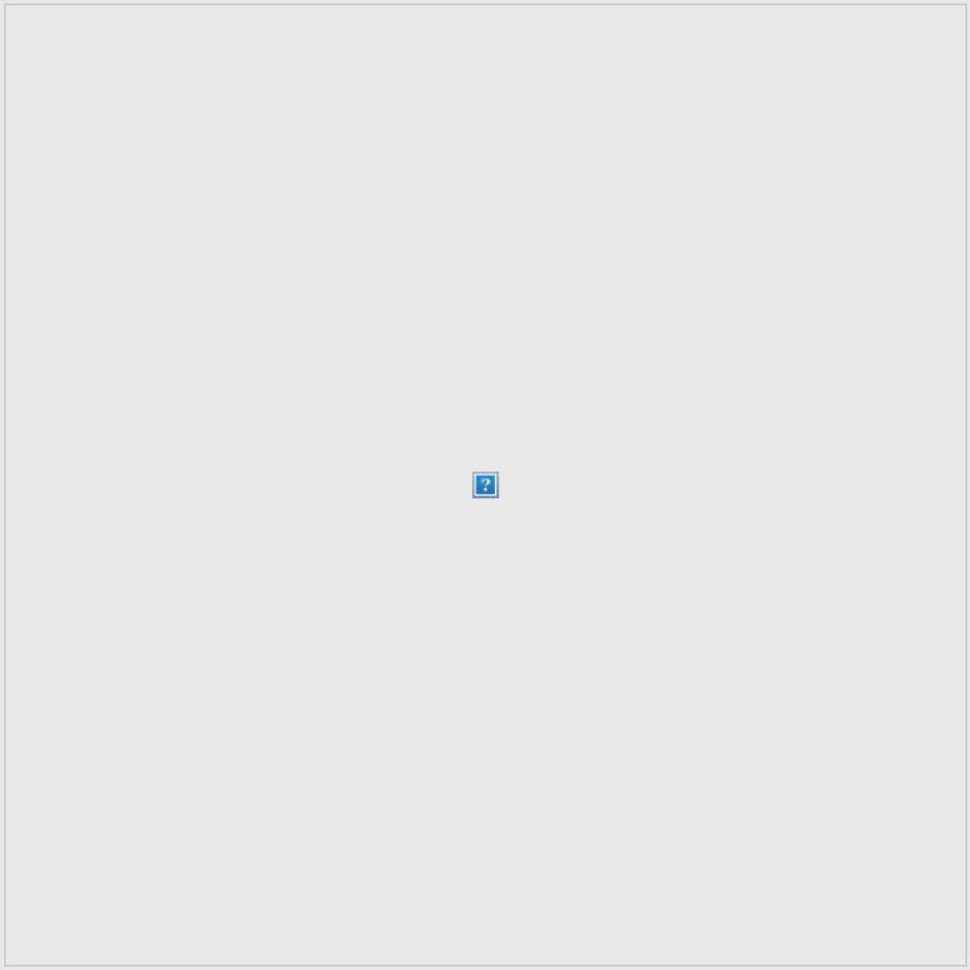
Bobit Business Media is located at 21250 Hawthorne Blvd, Suite 360, Torrance CA 90503

Contact Us | Privacy Policy | Unsubscribe

From: POLICE
To: McCarthy, Jeffrey (POL)
Subject: Get POLICE"s Top How-To"s
Date: Monday, April 3, 2023 12:33:40 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.

Apr 03, 2023



FREE WHITEPAPERS



Sponsored by Vector Solutions

CHECKLIST: Does Your Early Warning System Do These 4 Things?

Many of the early warning systems on the market today offer the same basic functionality for behavior tracking, use of force tracking, and other hot topics. Download this checklist to find out if your system has the right features.

DOWNLOAD



Raise the SCORE of Your Training Program

Progress comes with change, not complacency. Start impactful training now with SCORE.

DOWNLOAD



Sponsored by Collective Data

The Tennessee Department of Public Safety Increased Visibility, Accountability and Accuracy with Inventory Management Software Designed Specifically for Law Enforcement

Before implementing new software, TDPS was using spreadsheets alongside an outdated asset management system without flexibility to meet the department's needs resulting in many inefficiencies.

DOWNLOAD



Sponsored by POLICE, Adamson Industries, Traka USA/Assa Abloy

Special Report: Fleet Management Solutions

In this POLICE Special Report: "Fleet Management Solutions" read about some key issues in the maintenance and management of law enforcement vehicles. Learn 15 factors to consider when choosing an upfitter.

DOWNLOAD



Sponsored by POLICE

Special Report: Traffic Safety and Enforcement

Read about how e-citation systems are making traffic stops safer for officers and motorists, how motorists can work with police to report non-injury traffic accidents, how automatic license plate recognition (ALPR) systems can help agencies monitor traffic patterns, and how crash mapping can predict when and where accidents are likely to occur.

DOWNLOAD

POLICE MAGAZINE

You are currently subscribed as jeffrey mccarthy@pol.state.ma.us.

Bobit Business Media is located at 21250 Hawthorne Blvd, Suite 360, Torrance CA 90503

Contact Us | Privacy Policy | Unsubscribe

From: POLICE
To: McCarthy, Jeffrey (POL)
Subject: Get POLICE"s Top How-To"s
Date: Monday, March 6, 2023 12:33:37 PM

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

Mar 06, 2023

FREE WHITEPAPERS

Sponsored by Vector Solutions

Do You Practice These 3 Accountable Leadership Guidelines?

You are accountable to your officers, to the public, and to yourself. There is no one "right way" to be a leader, but providing the training and tools your officers need to get home safely is a good start. Learn more in this quick guide for leaders.

DOWNLOAD



Sponsored by VirTra

Raise the SCORE of Your Training Program

Progress comes with change, not complacency. Start impactful training now with SCORE.

DOWNLOAD



Sponsored by Collective Data

The Tennessee Department of Public Safety Increased Visibility, Accountability and Accuracy with Inventory Management Software Designed Specifically for Law Enforcement

Before implementing new software, TDPS was using spreadsheets alongside an outdated asset management system without flexibility to meet the department's needs resulting in many inefficiencies.

DOWNLOAD



Sponsored by POLICE, Adamson Industries, Traka USA/Assa Abloy

Special Report: Fleet Management Solutions

In this POLICE Special Report: "Fleet Management Solutions" read about some key issues in the maintenance and management of law enforcement vehicles. Learn 15 factors to consider when choosing an upfitter.

DOWNLOAD



Sponsored by POLICE

Special Report: Traffic Safety and Enforcement

Read about how e-citation systems are making traffic stops safer for officers and motorists, how motorists can work with police to report non-injury traffic accidents, how automatic license plate recognition (ALPR) systems can help agencies monitor traffic patterns, and how crash mapping can predict when and where accidents are likely to occur.

DOWNLOAD

Sponsored by Amplivox Sound Systems, BlueRidge Armor, Hardwire LLC, Johnson Controls, Nuance Communications, Ring Power

Special Report: Critical Incident Response

In POLICE Magazine's Special Report: Critical Incident Response, read about Working with the Media After a Critical Incident, the Evolution of Critical Incident Communications, Bomb Threats and Suspicious Packages, Preplanning Response to School Shootings, and PTSD in the Police K-9.

DOWNLOAD

POLICE MAGAZINE

You are currently subscribed as jeffrey mccarthy@pol.state.ma.us.

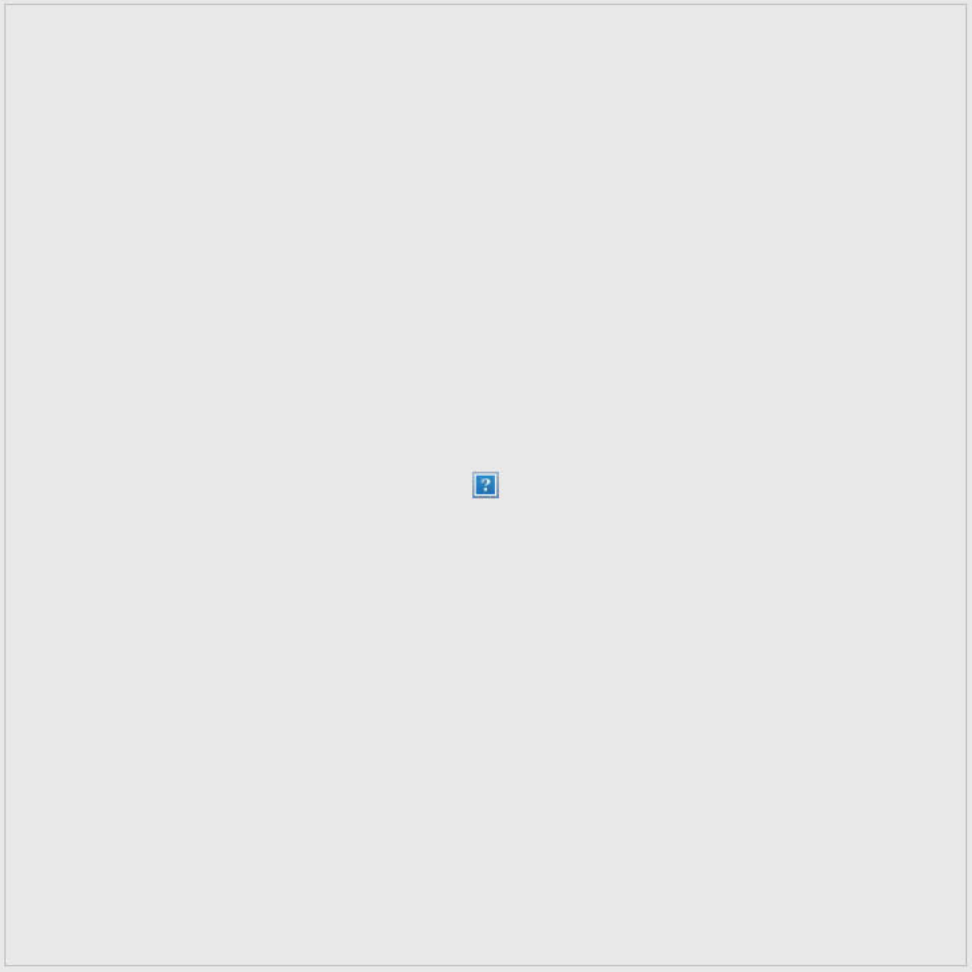
Bobit Business Media is located at 21250 Hawthorne Blvd, Suite 360, Torrance CA 90503

Contact Us | Privacy Policy | Unsubscribe

From: POLICE
To: McCarthy, Jeffrey (POL)
Subject: Get POLICE"s Top How-To"s
Date: Monday, May 15, 2023 12:33:57 PM

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

May 15, 2023



FREE WHITEPAPERS



Sponsored by POLICE, Leonardo & LexisNexis Coplogic

SPECIAL REPORT: Traffic Safety and Enforcement

In this POLICE Special Report: Traffic Safety and Enforcement, read about new technologies in accident prevention and roadway monitoring.

DOWNLOAD

Sponsored by Collective Data

The Tennessee Department of Public Safety Increased Visibility, Accountability and Accuracy with Inventory Management Software Designed Specifically for Law Enforcement

Before implementing new software, TDPS was using spreadsheets alongside an outdated asset management system without flexibility to meet the department's needs resulting in many inefficiencies.

DOWNLOAD

Sponsored by POLICE, Adamson Industries, Traka USA/Assa Abloy

Special Report: Fleet Management Solutions

In this POLICE Special Report: "Fleet Management Solutions" read about some key issues in the maintenance and management of law enforcement vehicles. Learn 15 factors to consider when choosing an upfitter.

DOWNLOAD

Sponsored by POLICE

Special Report: Traffic Safety and Enforcement

Read about how e-citation systems are making traffic stops safer for officers and motorists, how motorists can work with police to report non-injury traffic accidents, how automatic license plate recognition (ALPR) systems can help agencies monitor traffic patterns, and how crash mapping can predict when and where accidents are likely to occur.

DOWNLOAD

POLICE MAGAZINE

You are currently subscribed as jeffrey mccarthy@pol.state.ma.us.

Bobit Business Media is located at 21250 Hawthorne Blvd, Suite 360, Torrance CA 90503

Contact | Privacy | Unsubscribe

	Us	Policy

From: OFFICER Magazine
To: zzWildgrube, Danial (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:14:17 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.

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

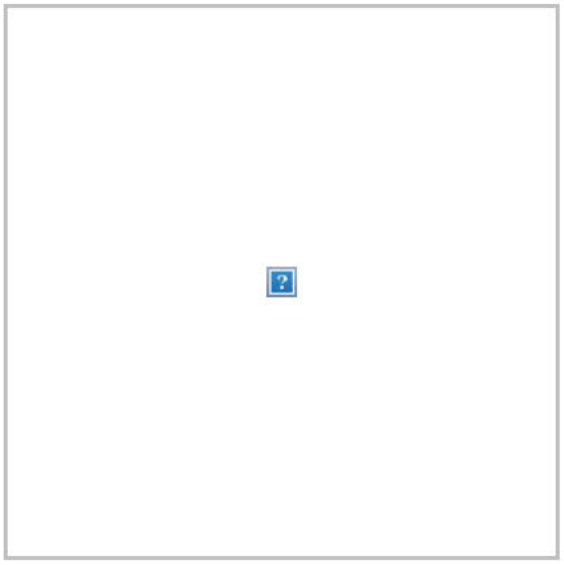
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

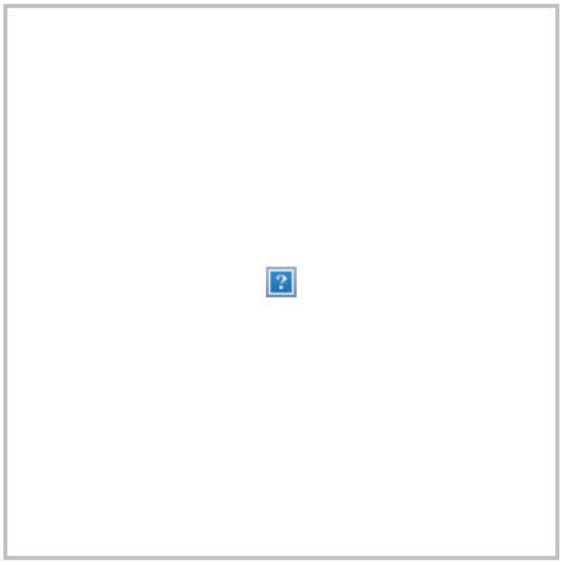
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



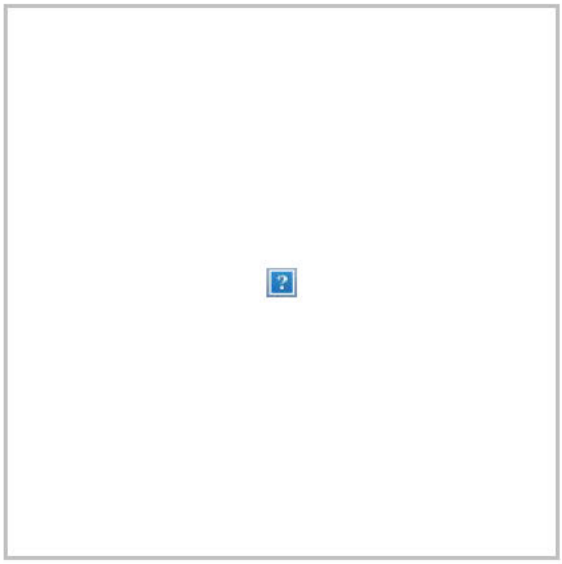
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



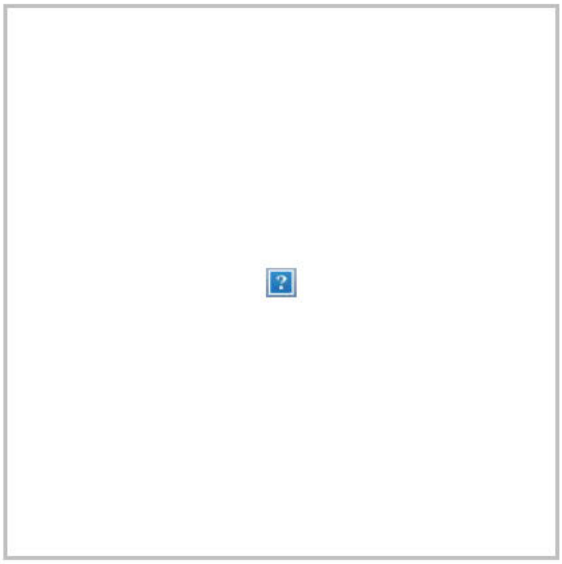
V-VICTA

One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

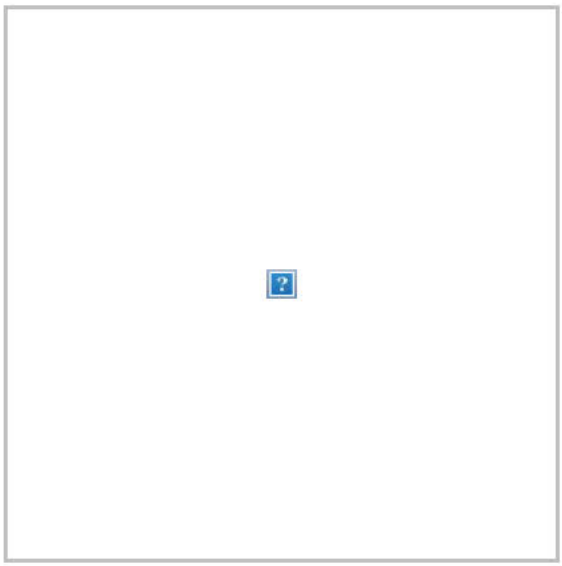
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...



Setina Rear Cargo Storage Box

Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

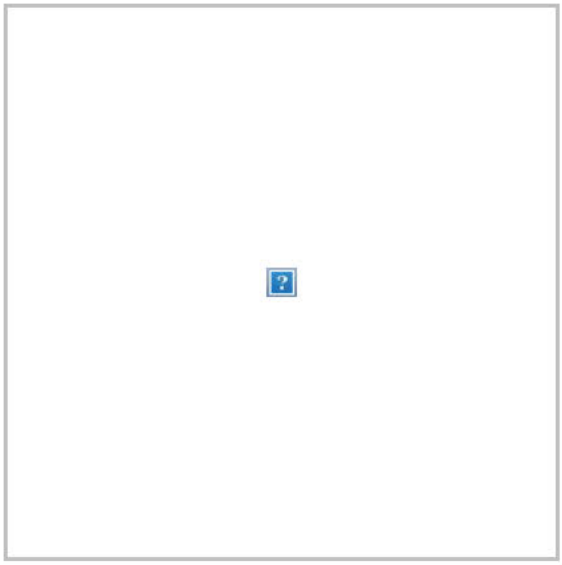
NEW PRODUCTS



Flock Safety Raven

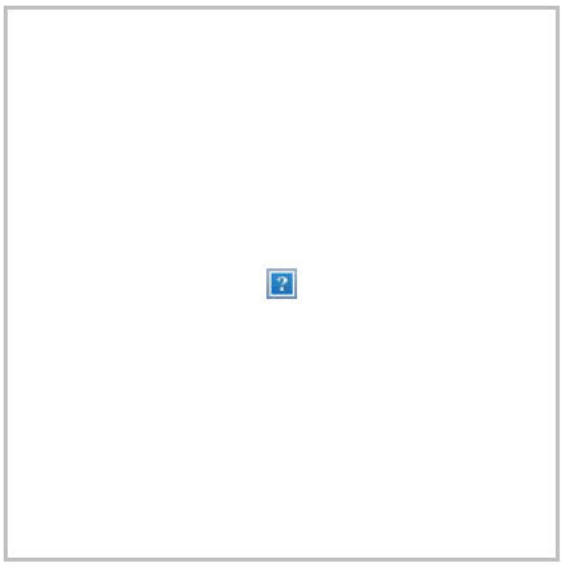
The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem

with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

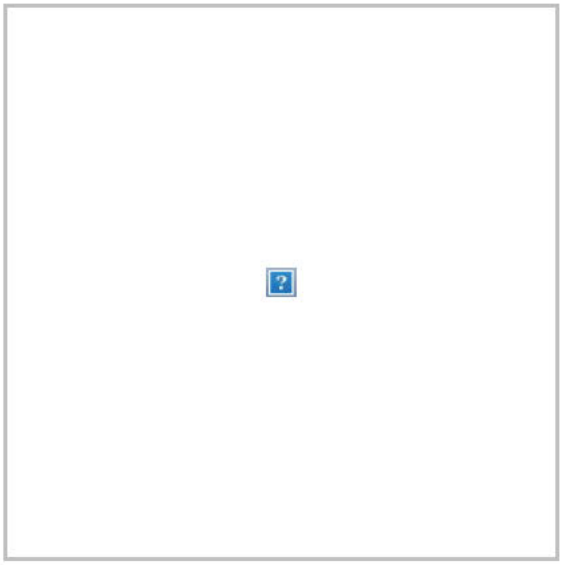


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



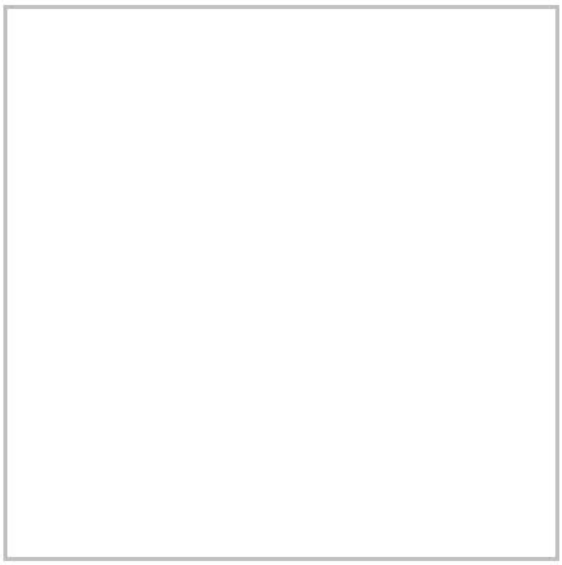
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

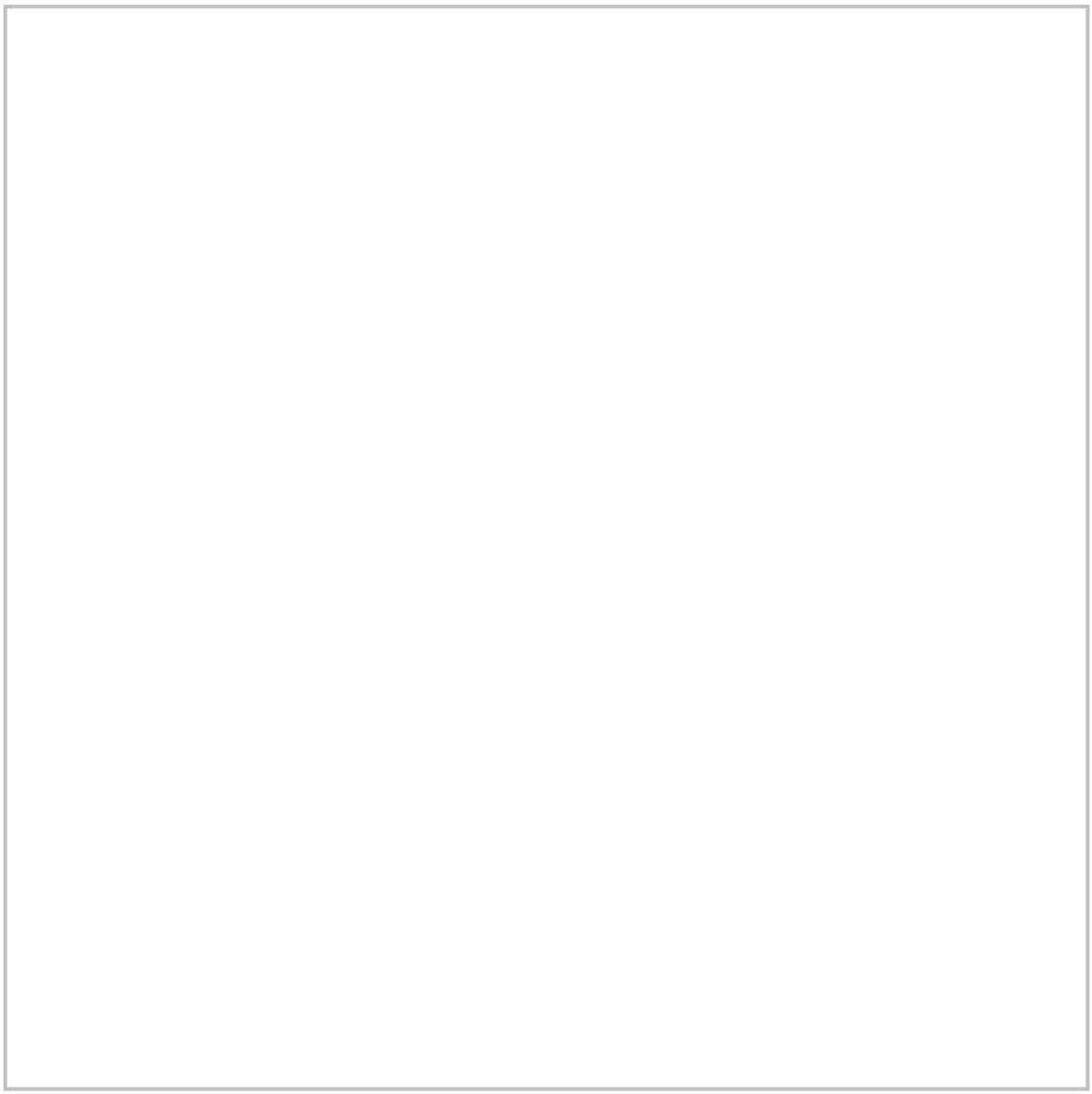
The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE



Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.



Let's Talk Holsters

When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

Integrating Technology: Juggling Public Safety Mission with High-Tech



2023 Uniform Trends

What law enforcement agencies are buying and what new products to watch.

Going Digital: Harnessing Digital Forensics Technology

The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.

As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION

Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us

This email is being sent to danial.wildgrube@pol.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: Barstow, Matthew (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:10:17 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.

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

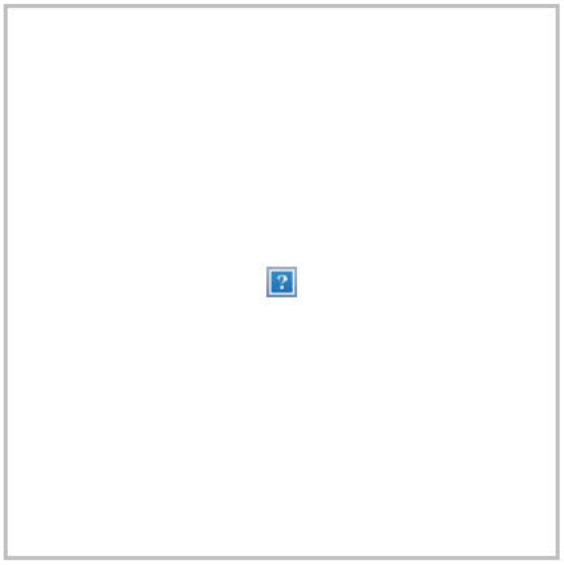
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

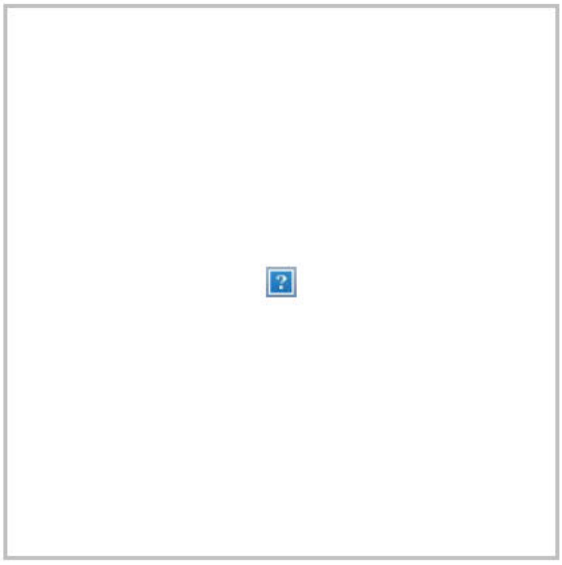
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



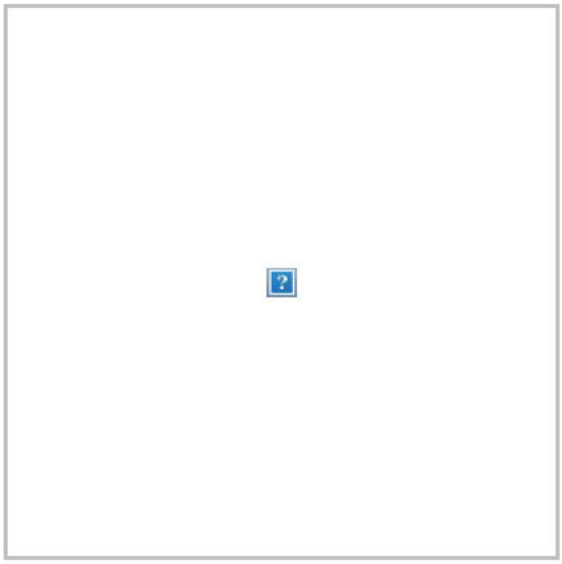
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



V-VICTA

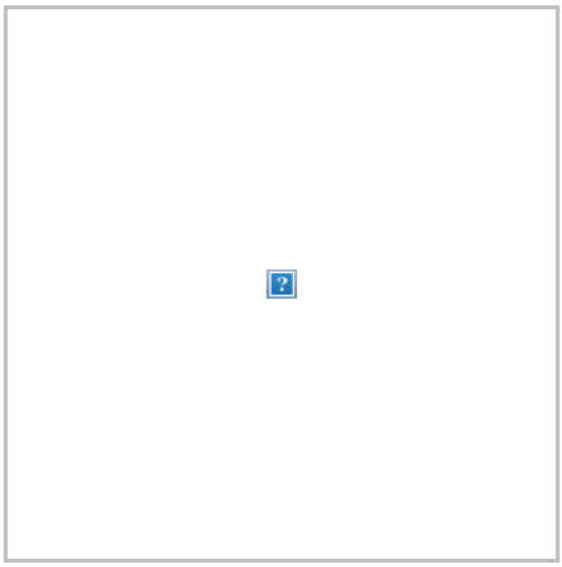
One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

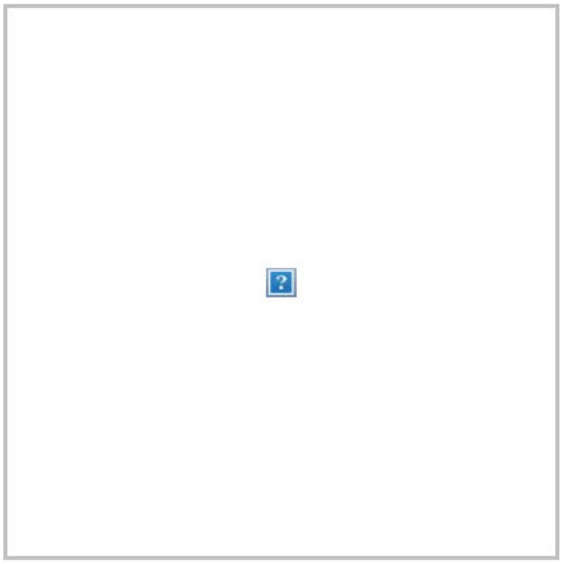
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...

NEW PRODUCTS



Flock Safety Raven

The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem

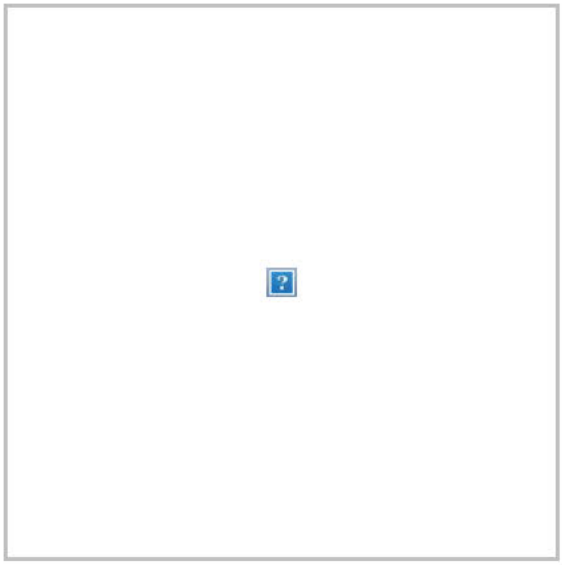


Setina Rear Cargo Storage Box

Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

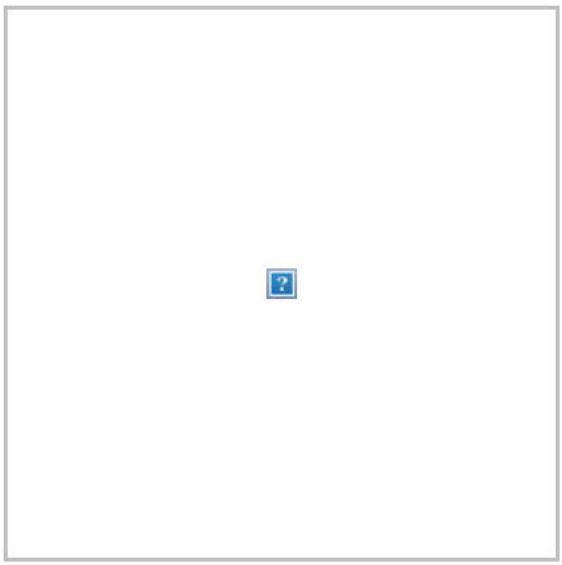


with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

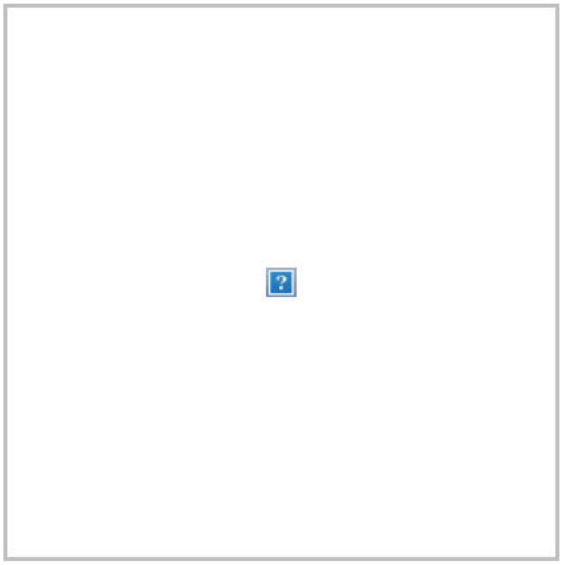


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



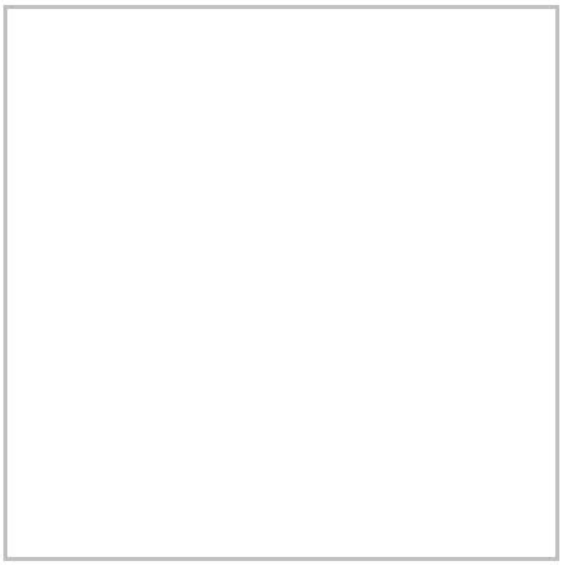
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

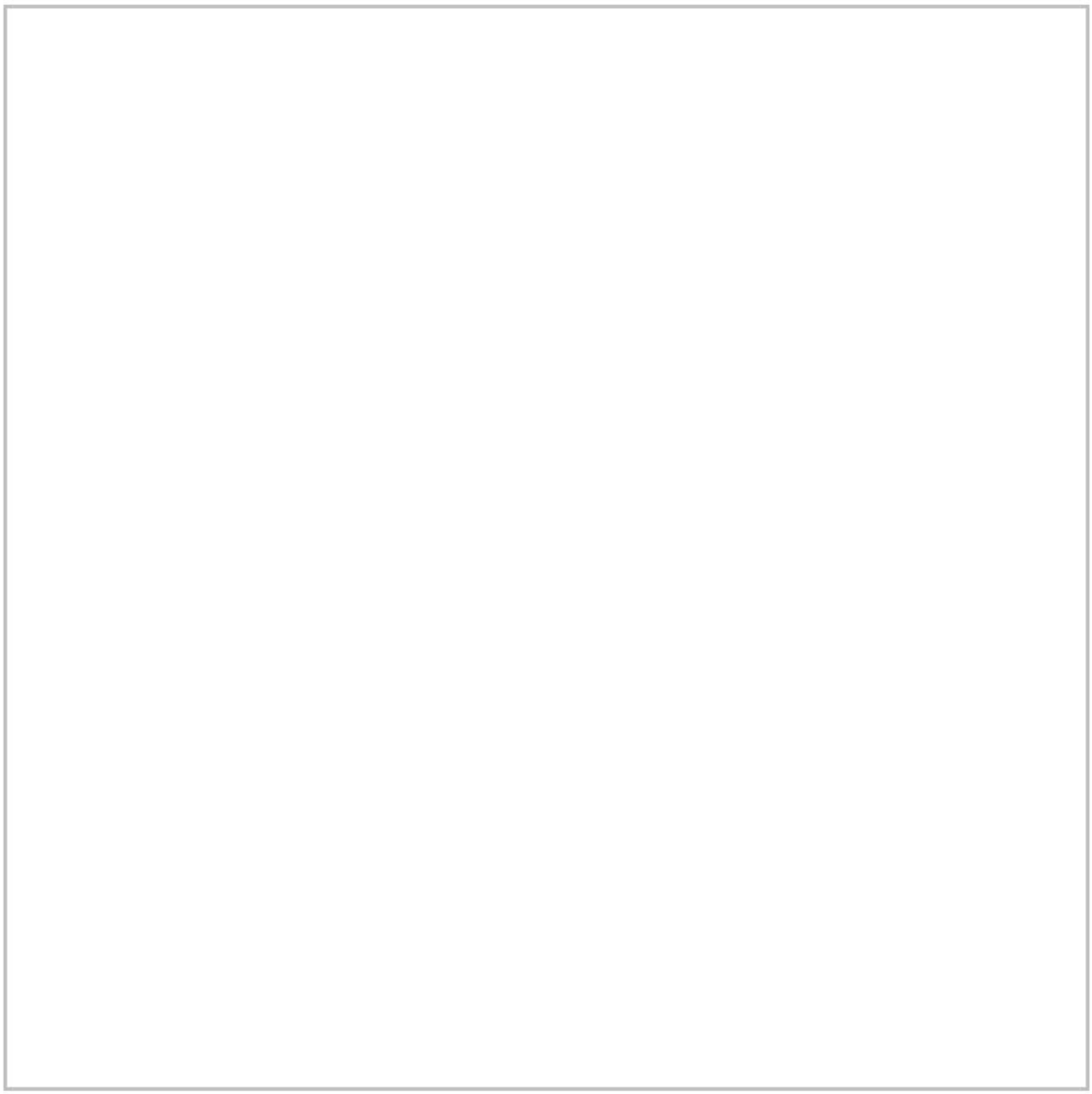
The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE



Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.



Let's Talk Holsters

When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

Integrating Technology: Juggling Public Safety Mission with High-Tech



2023 Uniform Trends

What law enforcement agencies are buying and what new products to watch.

Going Digital: Harnessing Digital Forensics Technology

The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.

As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION

Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us

This email is being sent to matthew.barstow@mass.gov.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: Fletcher, Marion (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:10:00 PM

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

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

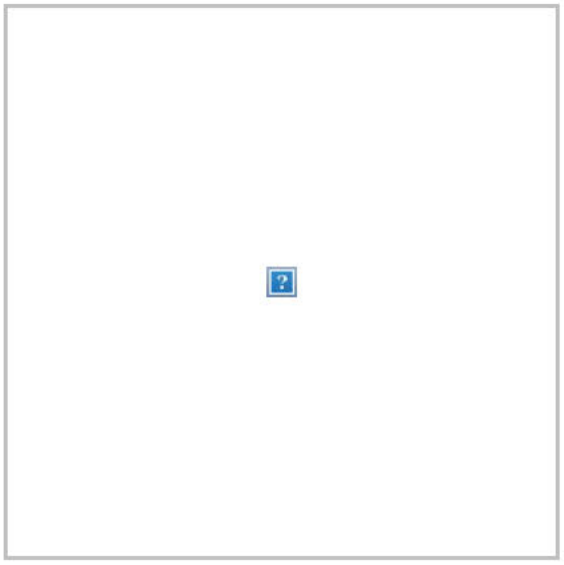
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

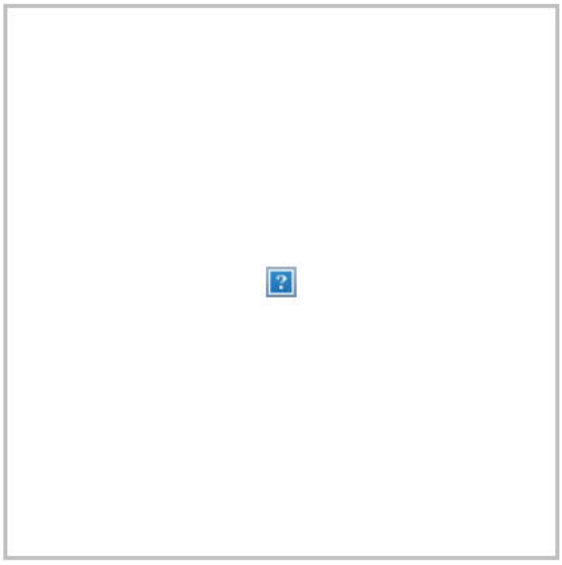
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



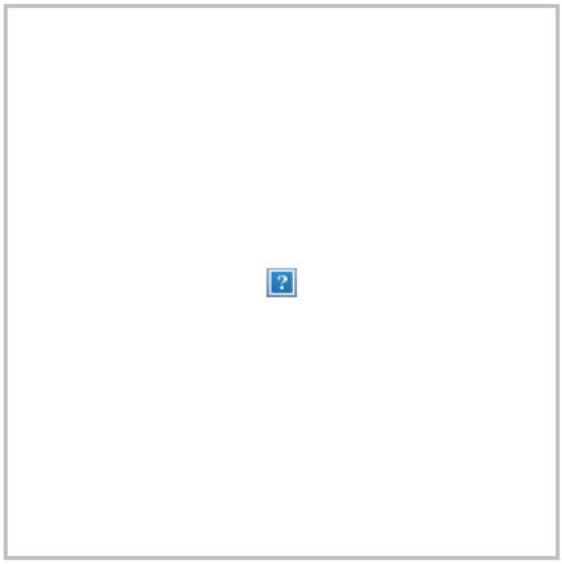
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



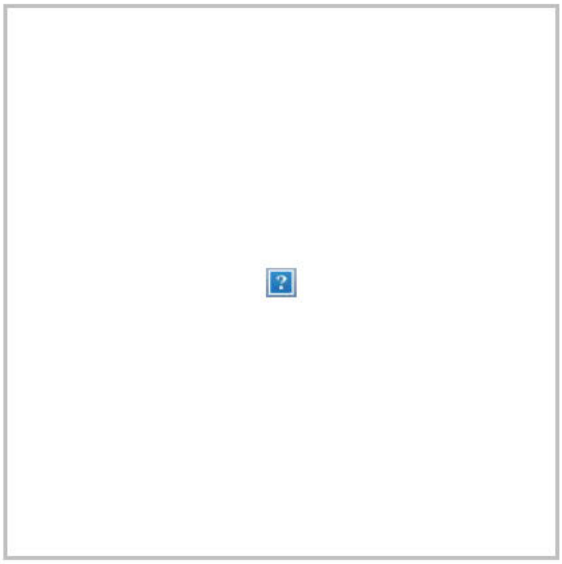
V-VICTA

One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

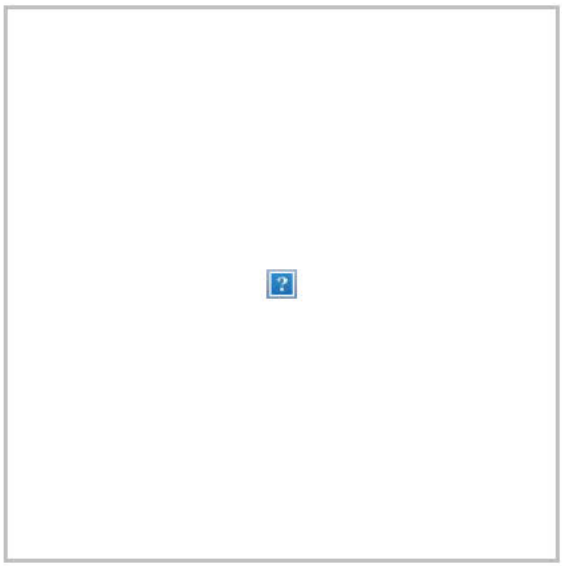
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...



Setina Rear Cargo Storage Box

Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

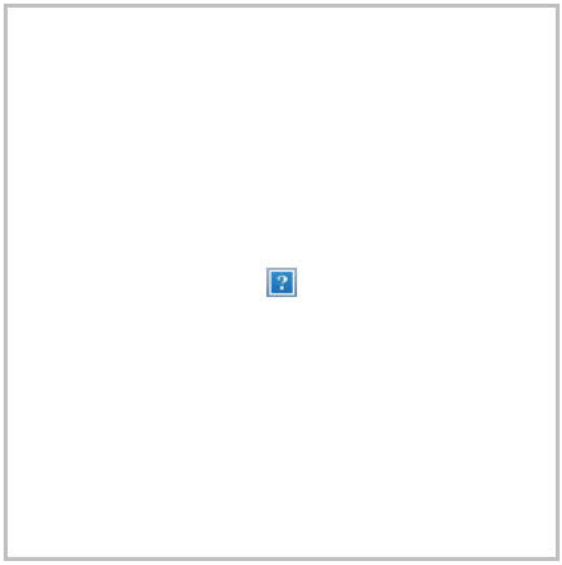
NEW PRODUCTS



Flock Safety Raven

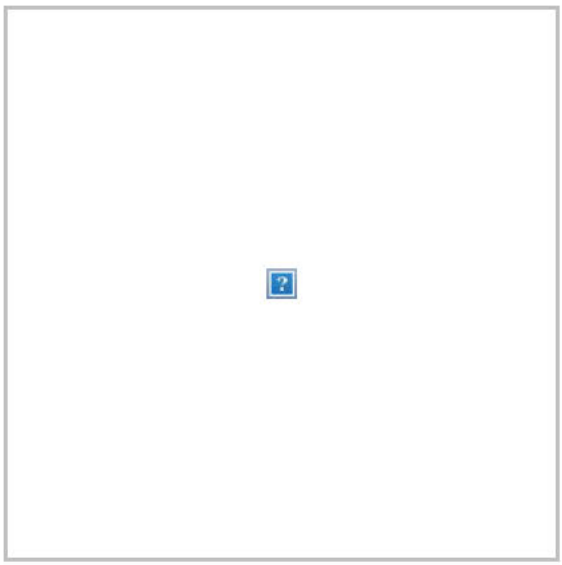
The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem

with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

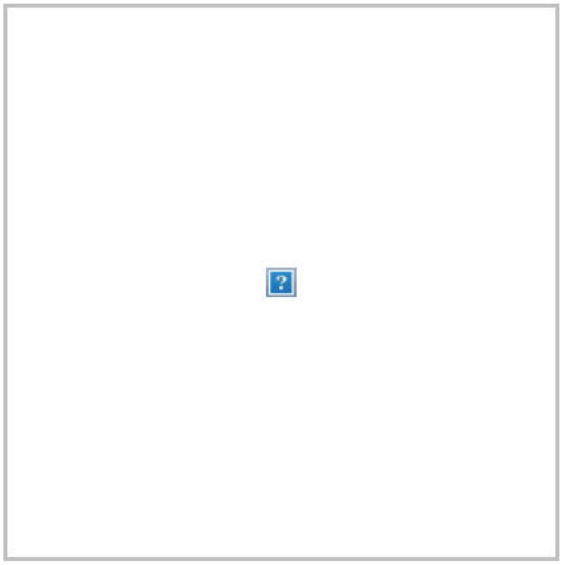


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



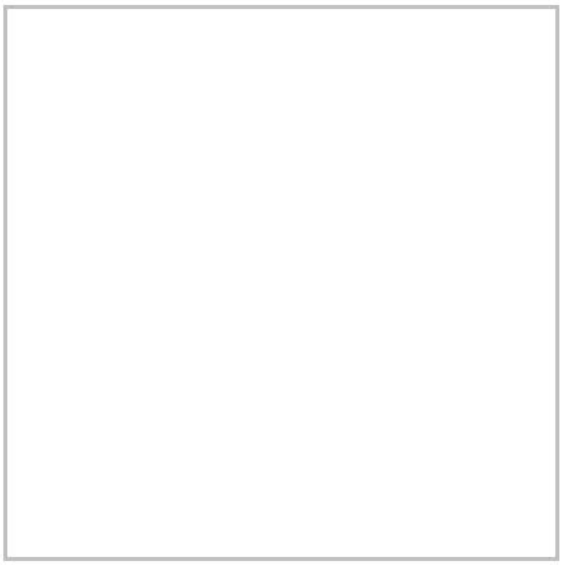
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE

Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.

Let's Talk Holsters

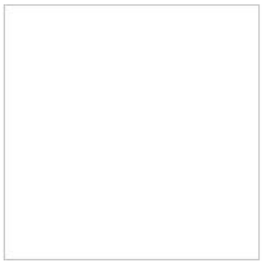
When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

2023 Uniform Trends

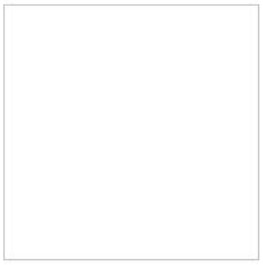
What law enforcement agencies are buying and what new products to watch.

Integrating Technology: Juggling Public Safety Mission with High-Tech

Going Digital: Harnessing Digital Forensics Technology

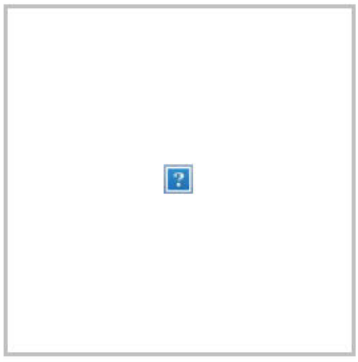


The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.



As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION



Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us



This email is being sent to marion.fletcher@pol.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: zzMichno, Michael (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:09:13 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.

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

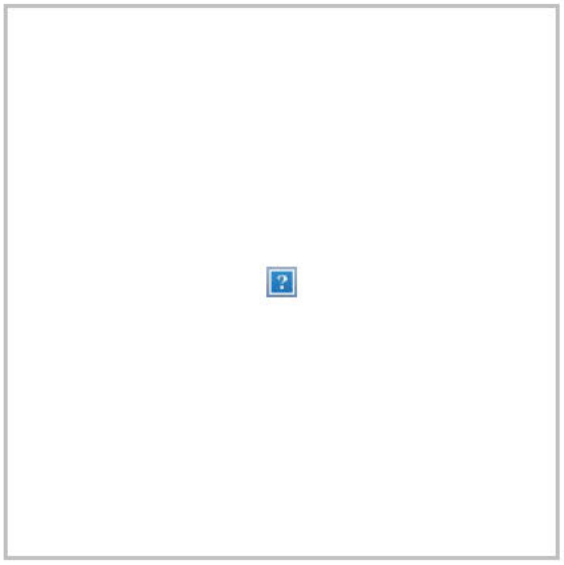
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

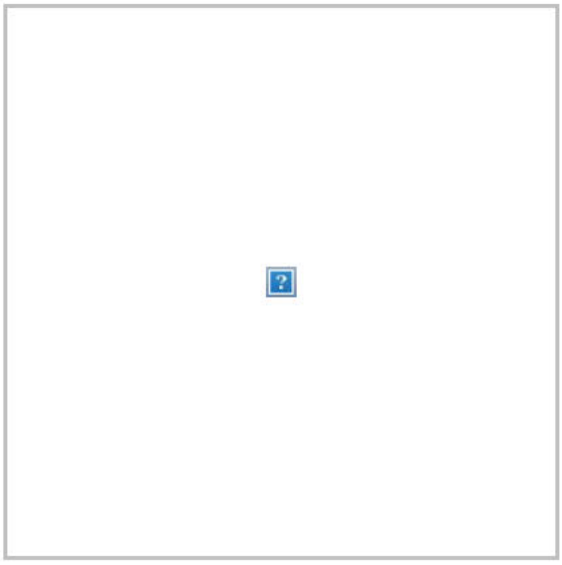
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



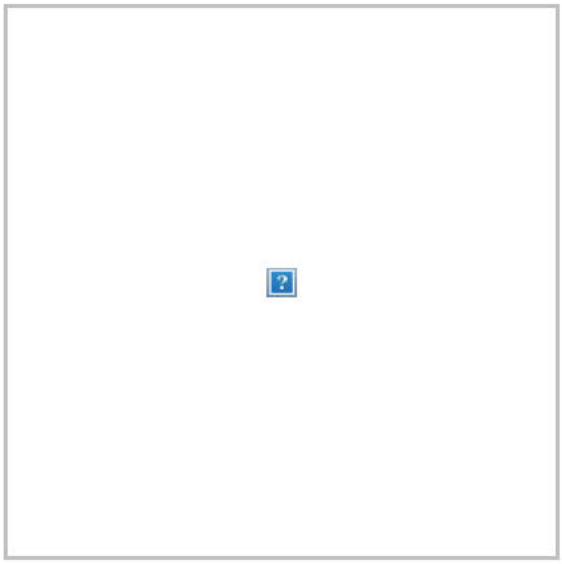
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



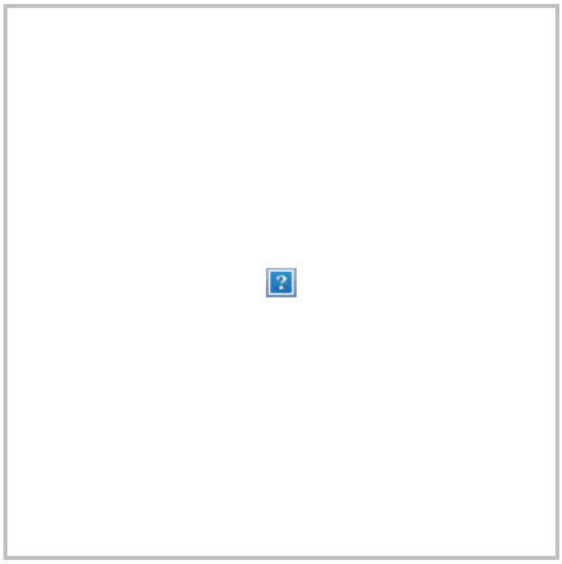
V-VICTA

One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

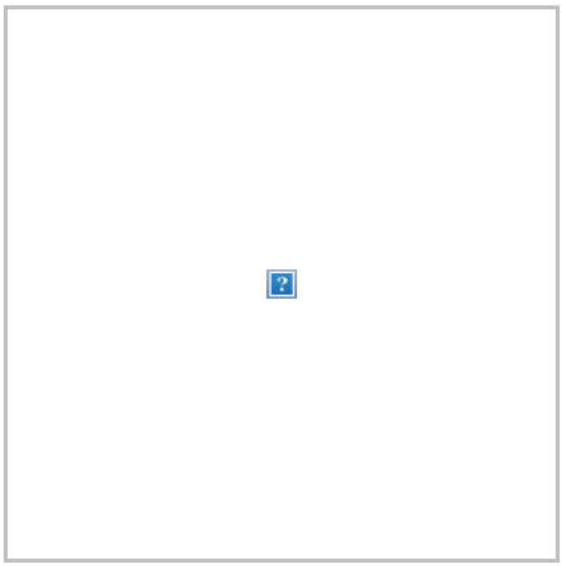
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...



Setina Rear Cargo Storage Box

Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

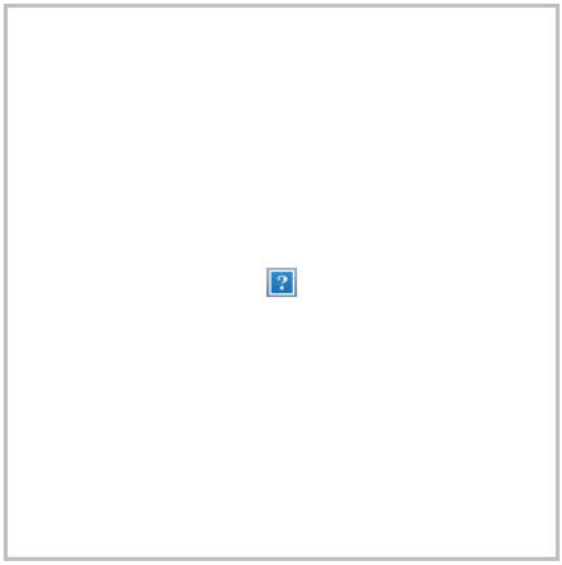
NEW PRODUCTS



Flock Safety Raven

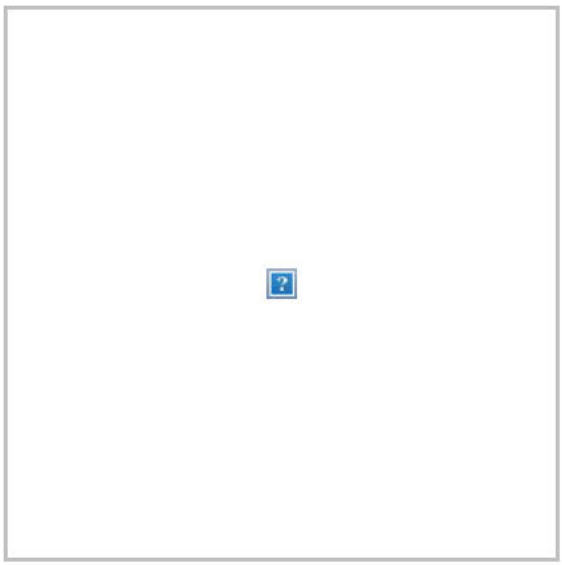
The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem

with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

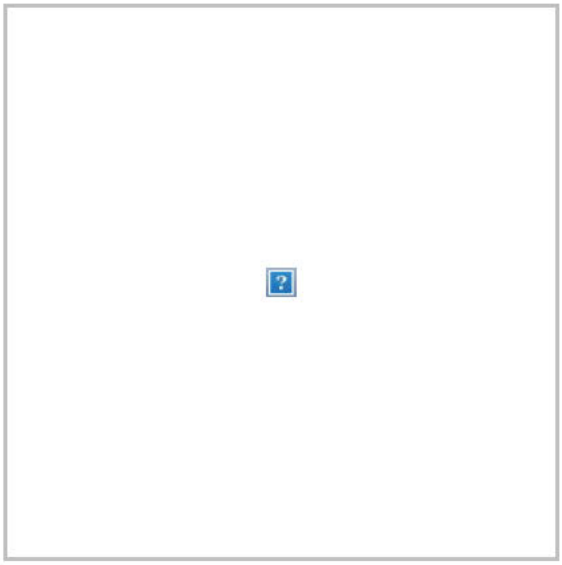


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



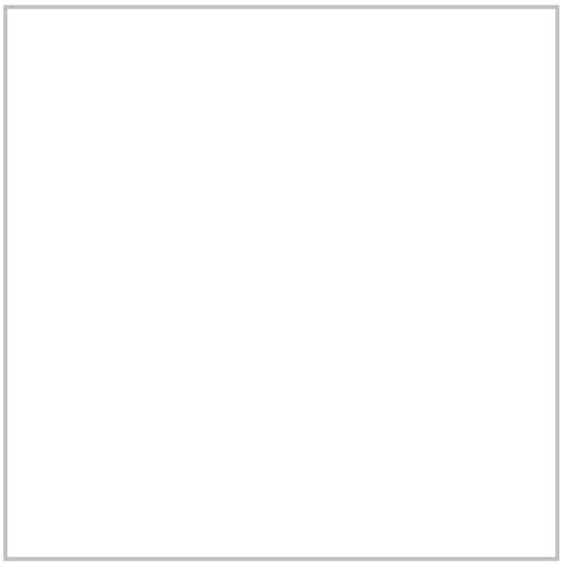
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

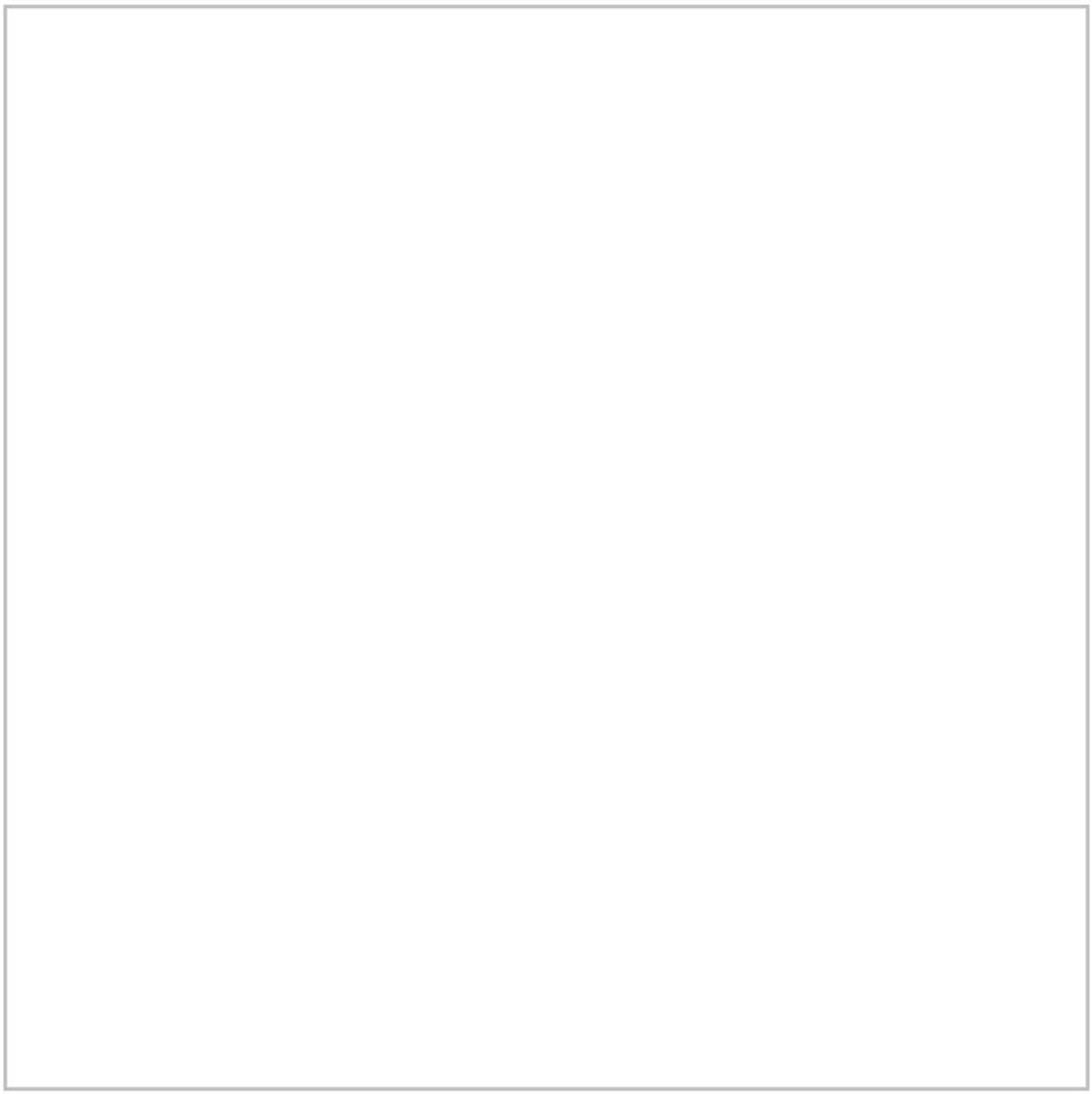
The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE



Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.



Let's Talk Holsters

When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

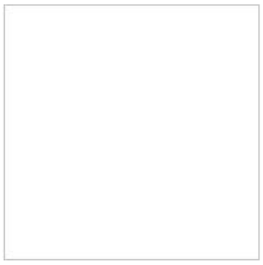
Integrating Technology: Juggling Public Safety Mission with High-Tech



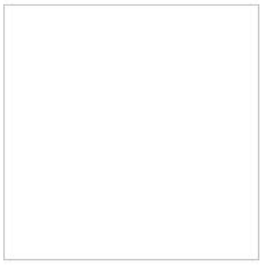
2023 Uniform Trends

What law enforcement agencies are buying and what new products to watch.

Going Digital: Harnessing Digital Forensics Technology

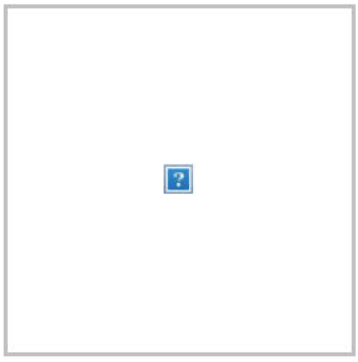


The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.



As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION



Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us



This email is being sent to michael.michno@pol.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: Sullivan, Thomas W (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:09:01 PM

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

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

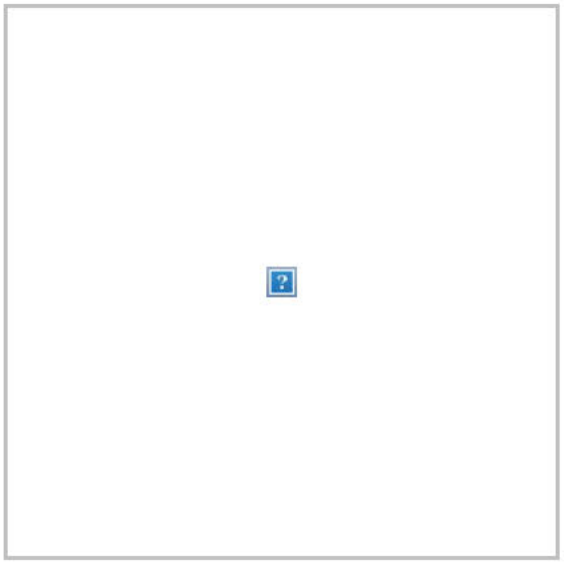
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

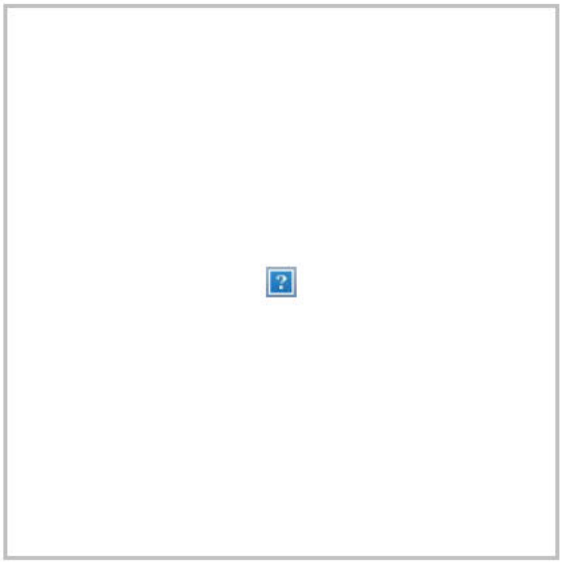
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



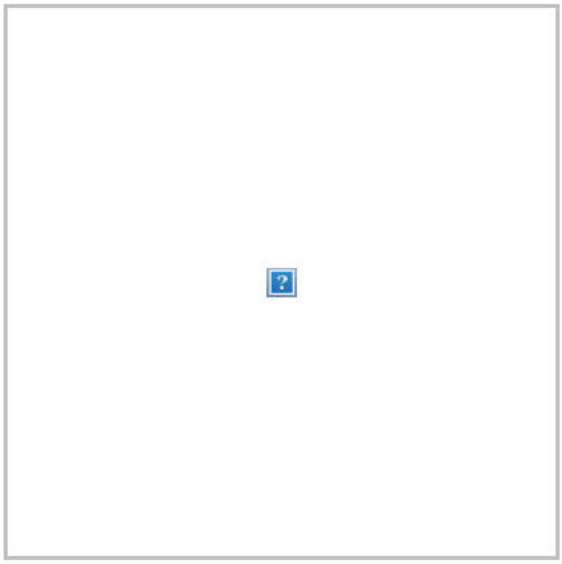
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



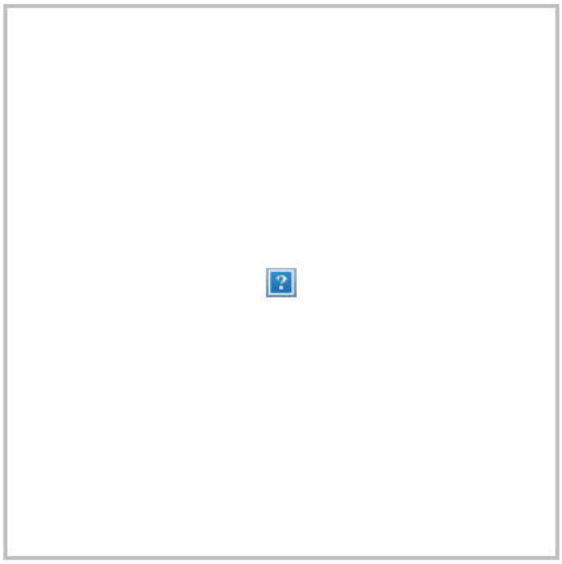
V-VICTA

One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

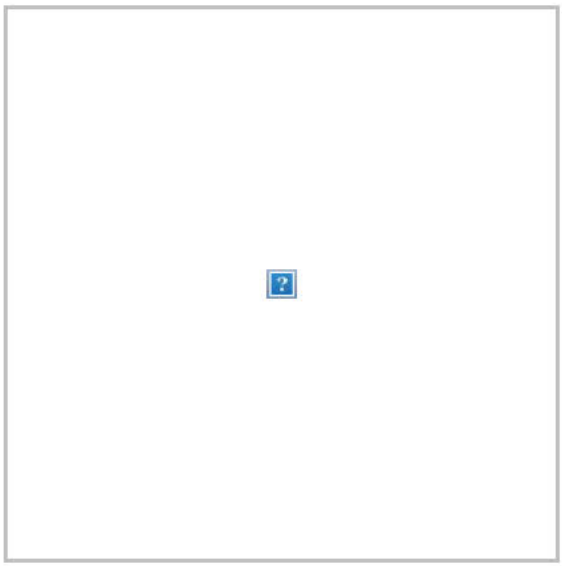
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...



Setina Rear Cargo Storage Box

Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

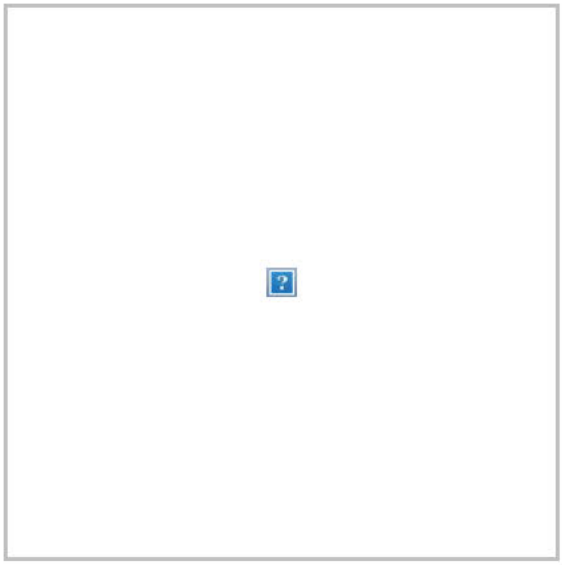
NEW PRODUCTS



Flock Safety Raven

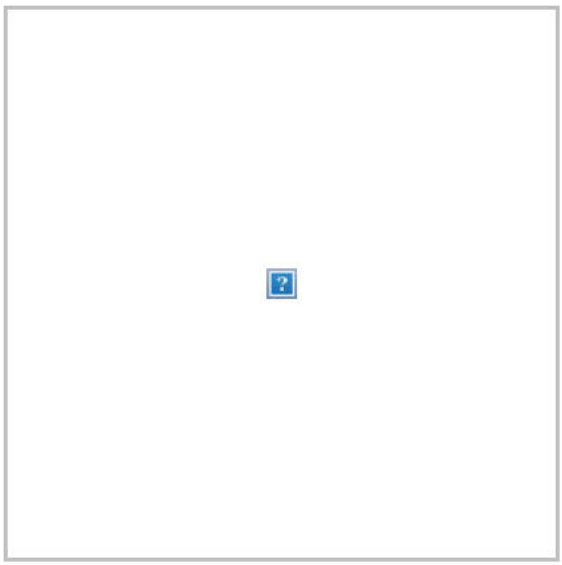
The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem

with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

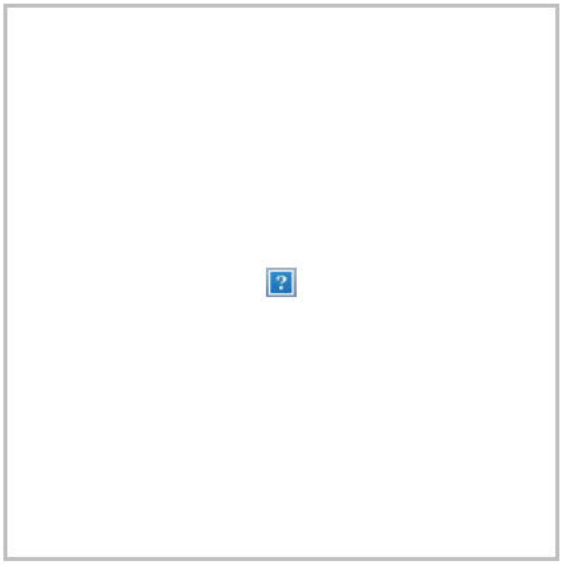


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



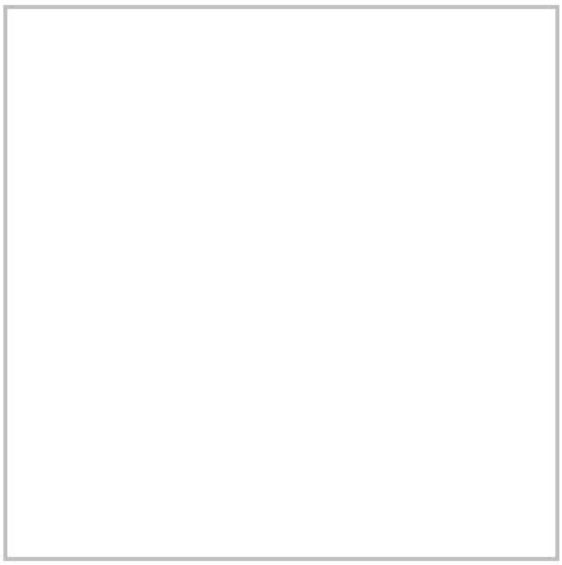
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE

Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.

Let's Talk Holsters

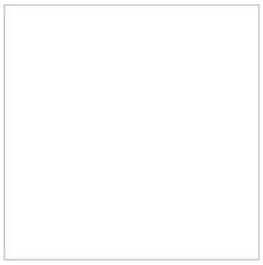
When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

2023 Uniform Trends

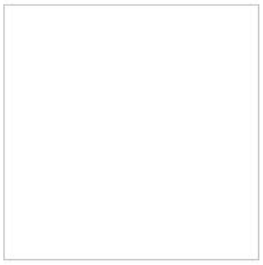
What law enforcement agencies are buying and what new products to watch.

Integrating Technology: Juggling Public Safety Mission with High-Tech

Going Digital: Harnessing Digital Forensics Technology

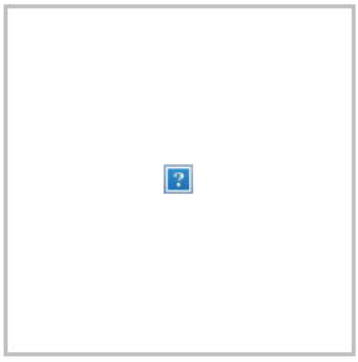


The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.



As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION



Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us



This email is being sent to thomas.w.sullivan3@massmail.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: Grassia, Michael (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:08:56 PM

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

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

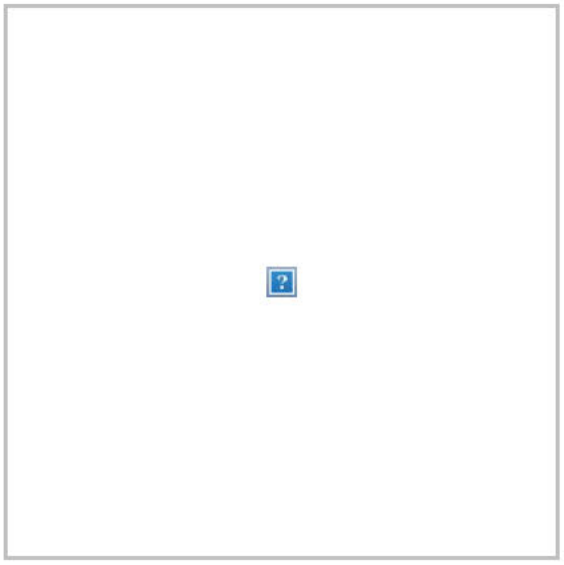
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

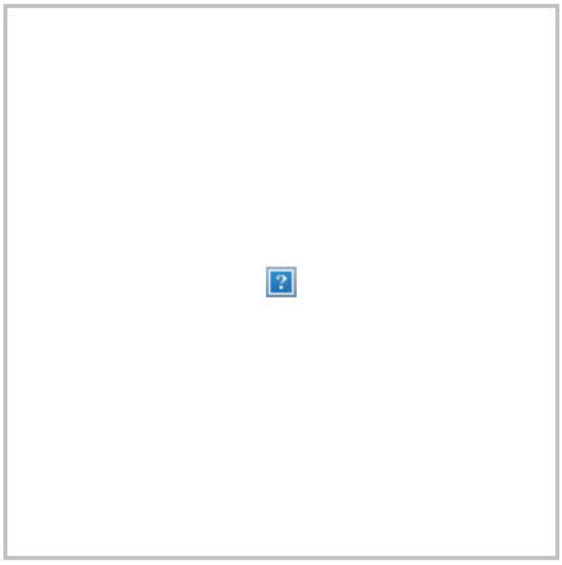
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



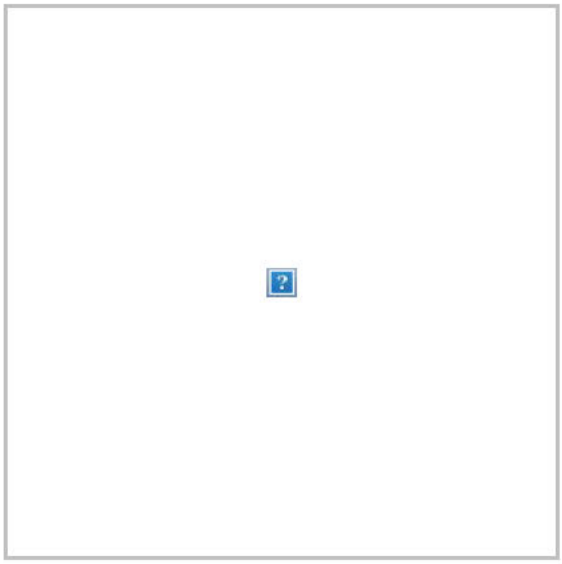
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



V-VICTA

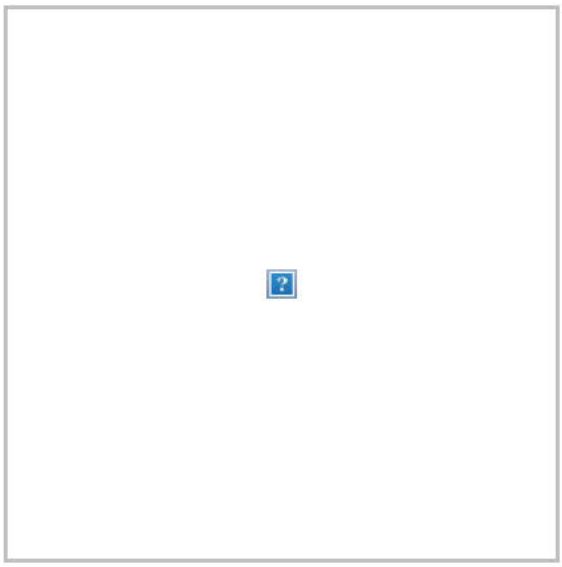
One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

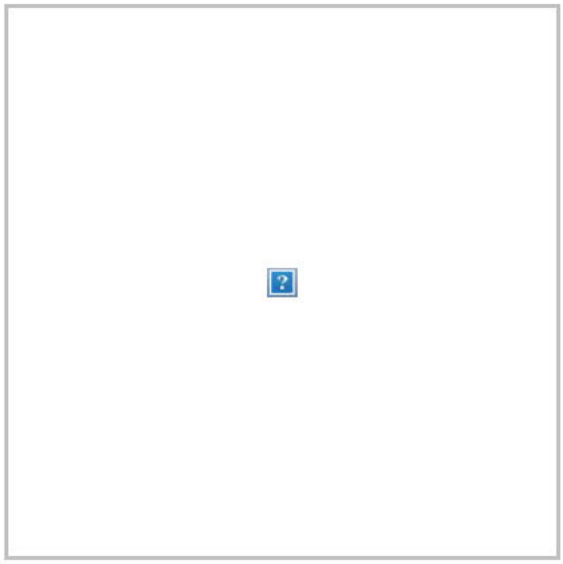
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...

NEW PRODUCTS



Flock Safety Raven

The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem

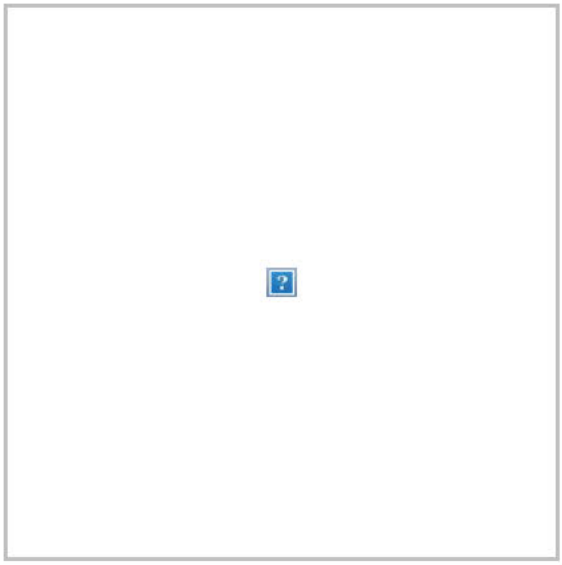


Setina Rear Cargo Storage Box

Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

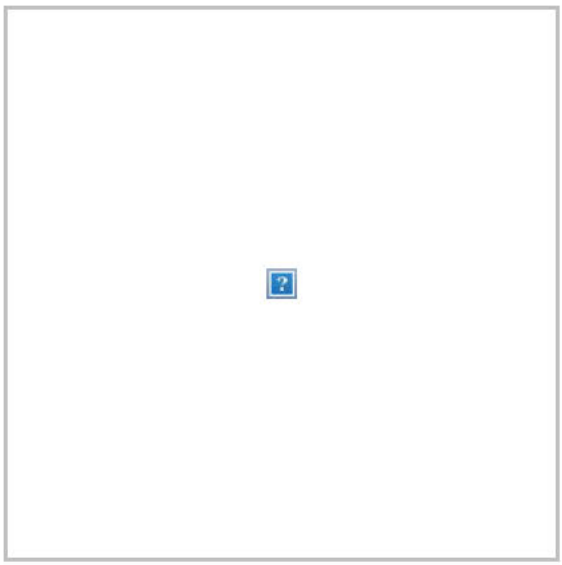


with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

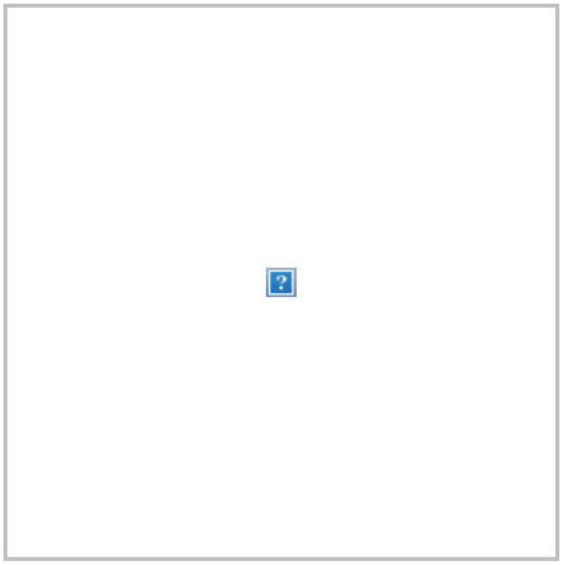


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



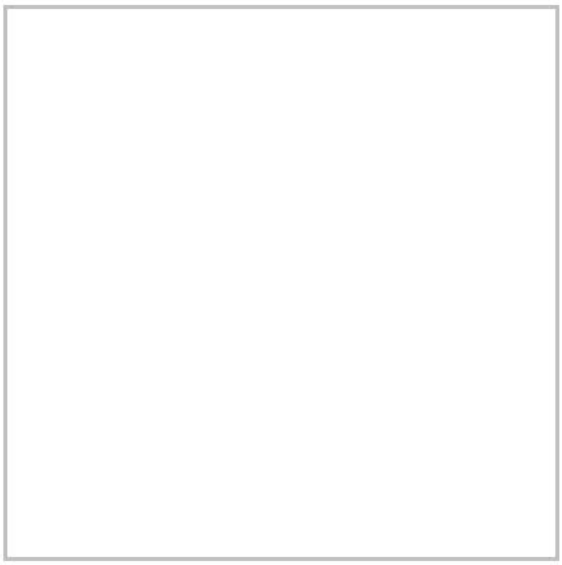
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

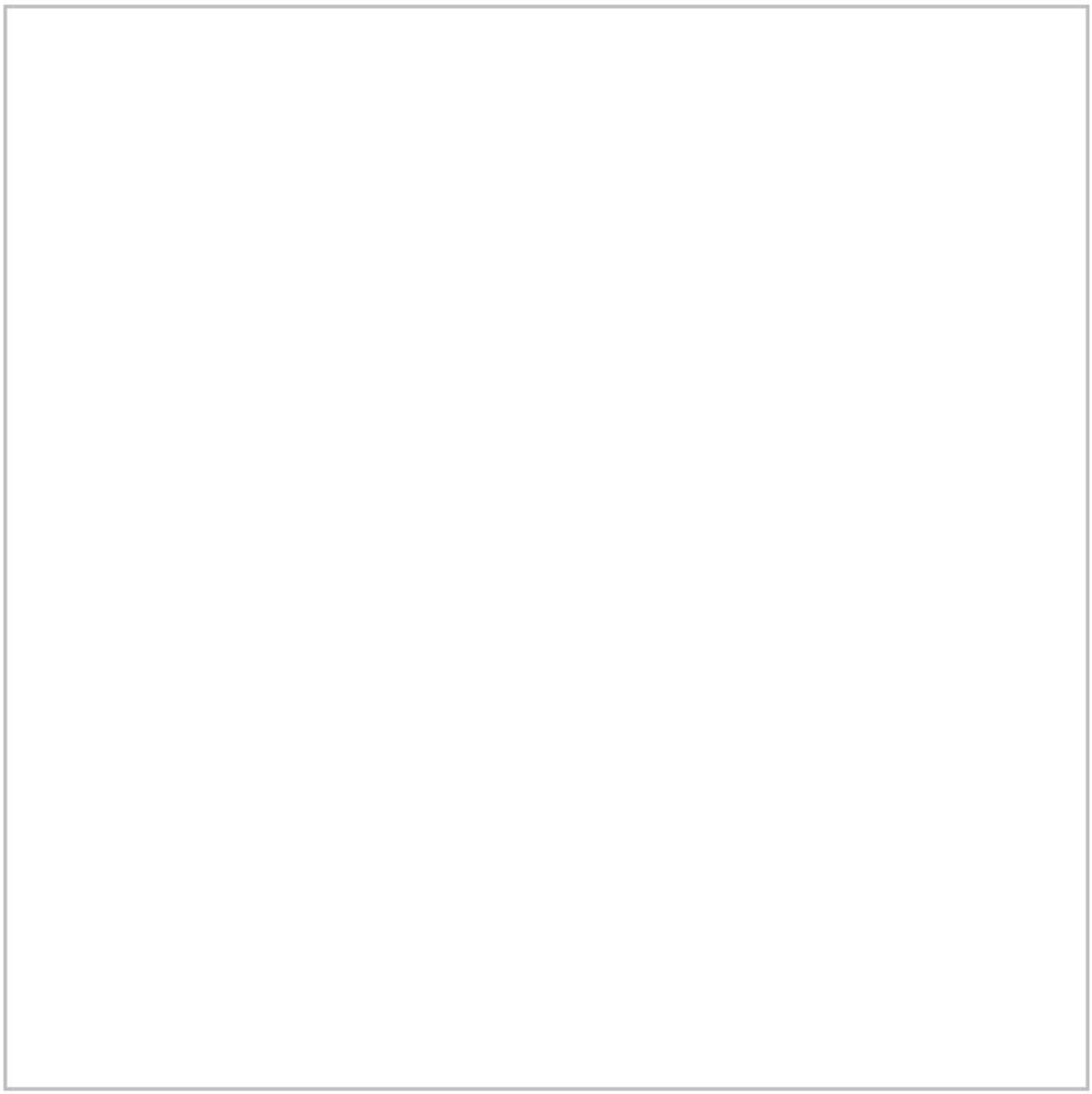
The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE



Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.



Let's Talk Holsters

When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

Integrating Technology: Juggling Public Safety Mission with High-Tech



2023 Uniform Trends

What law enforcement agencies are buying and what new products to watch.

Going Digital: Harnessing Digital Forensics Technology

The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.

As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION

Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us

This email is being sent to michael.grassia@pol.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: Flynn, Jack (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:08:37 PM

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

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

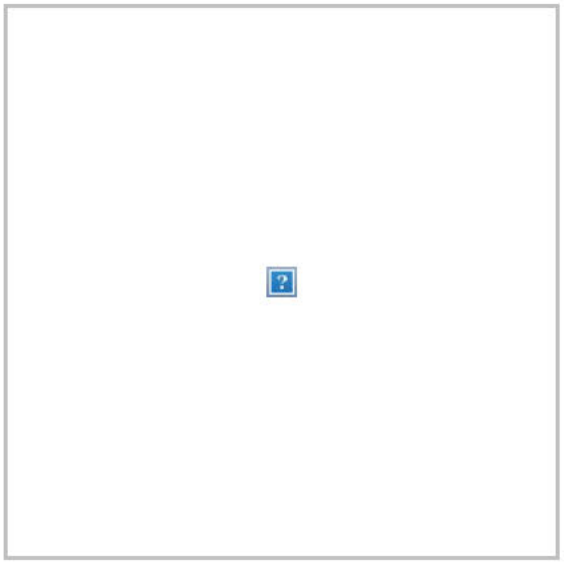
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

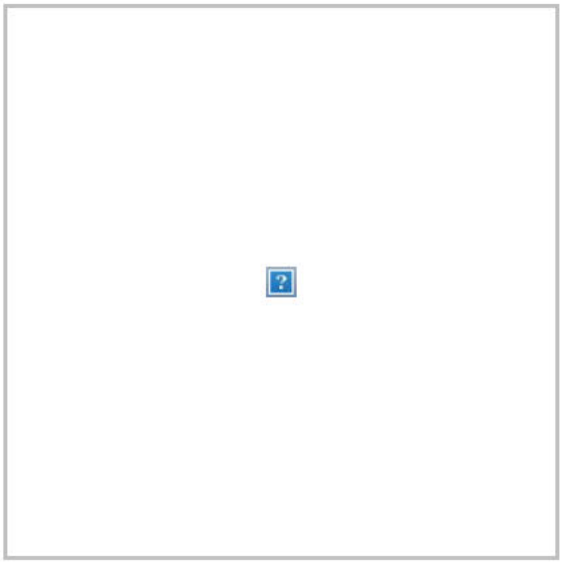
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



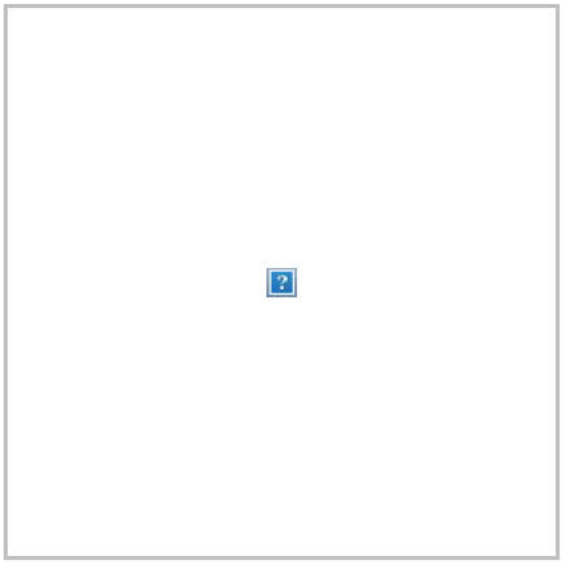
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



V-VICTA

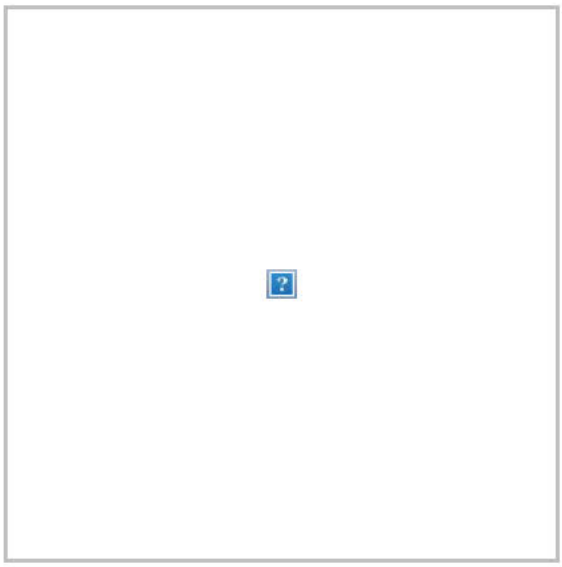
One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

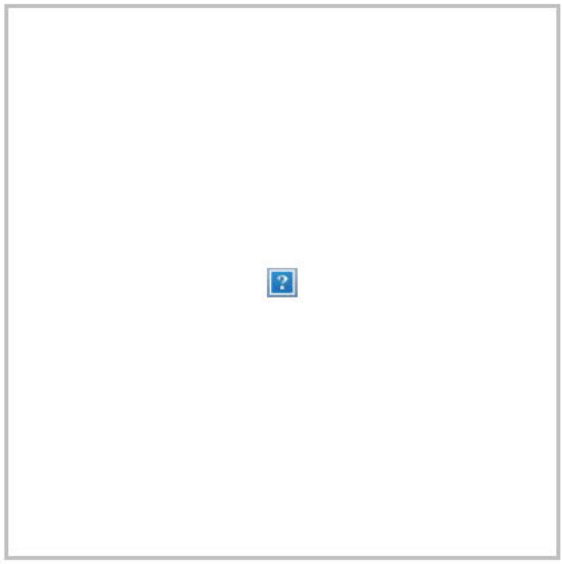
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...

NEW PRODUCTS



Flock Safety Raven

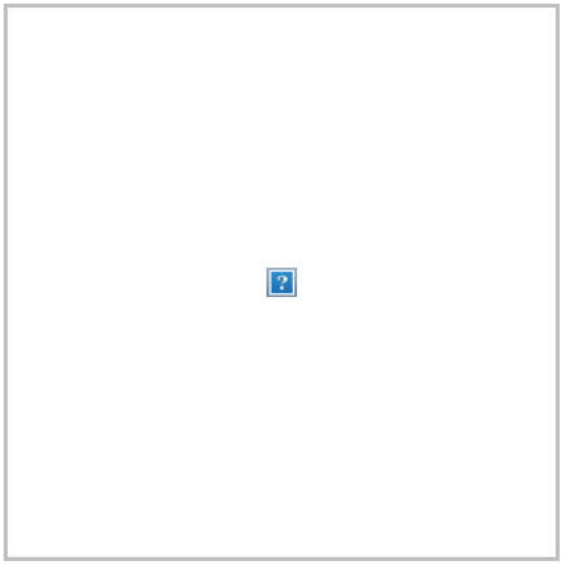
The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem



Setina Rear Cargo Storage Box

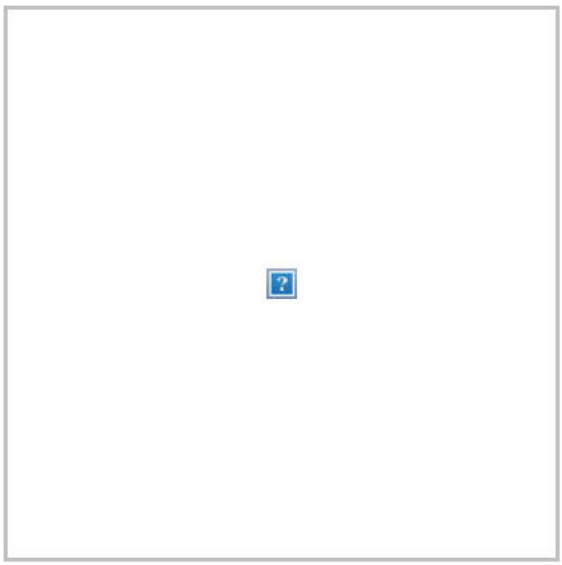
Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

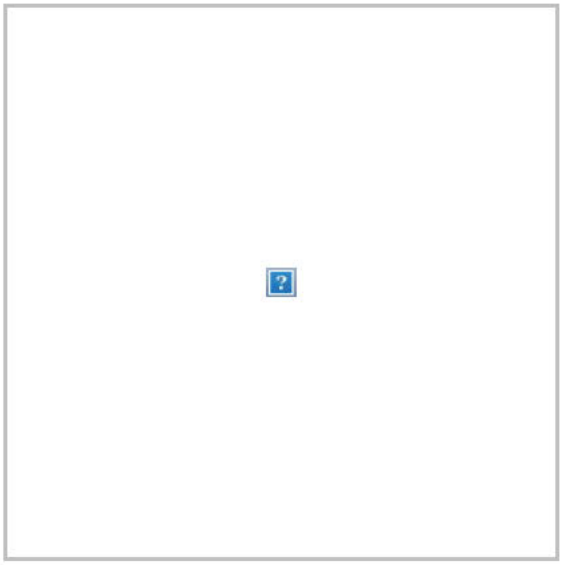


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



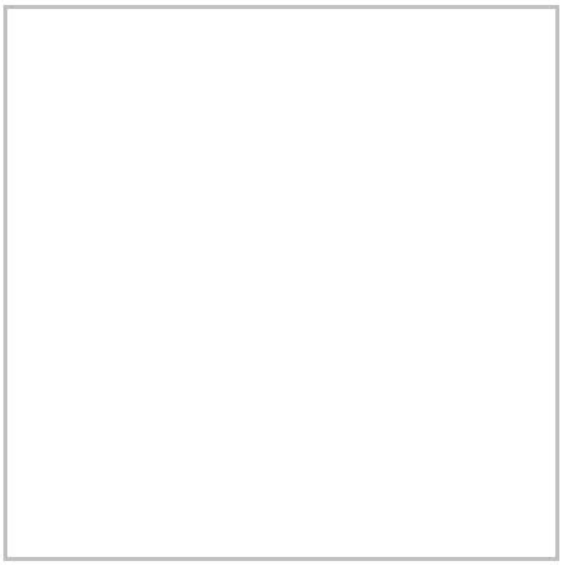
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE

Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.

Let's Talk Holsters

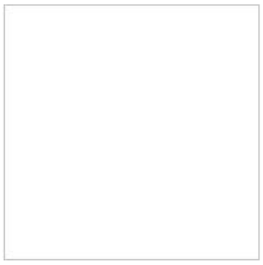
When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

2023 Uniform Trends

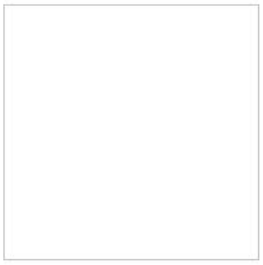
What law enforcement agencies are buying and what new products to watch.

Integrating Technology: Juggling Public Safety Mission with High-Tech

Going Digital: Harnessing Digital Forensics Technology

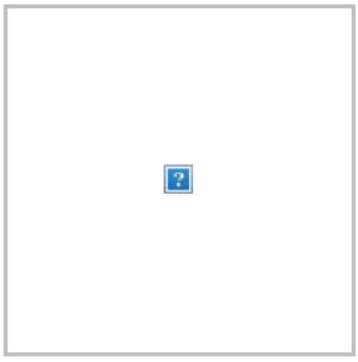


The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.



As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION



Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us



This email is being sent to jack.f.flynn@massmail.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: Blackwell, Edward (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:08:36 PM

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

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

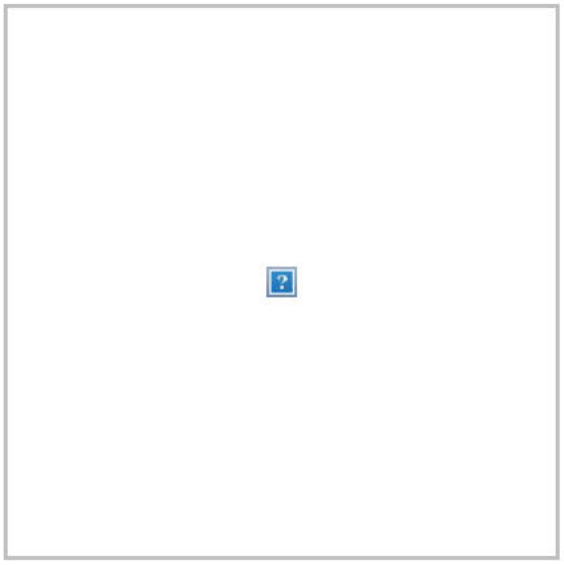
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

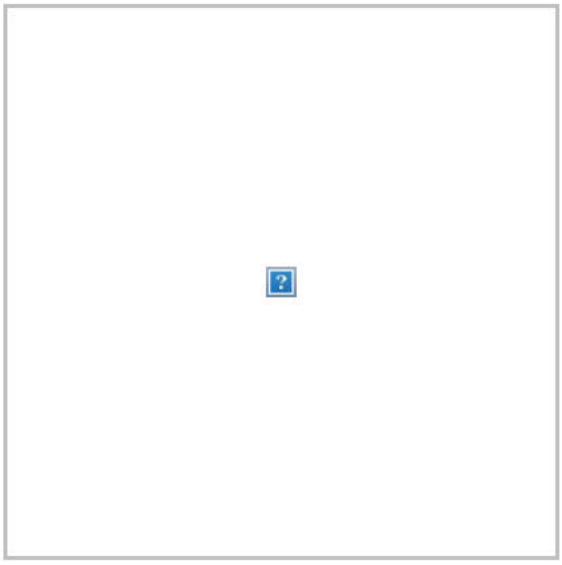
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



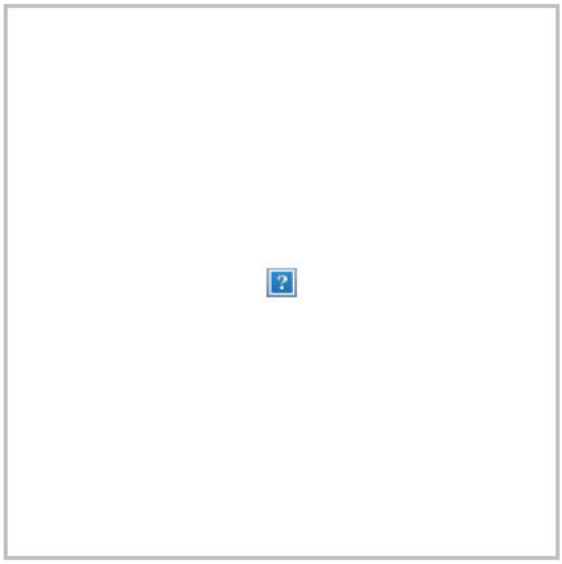
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



V-VICTA

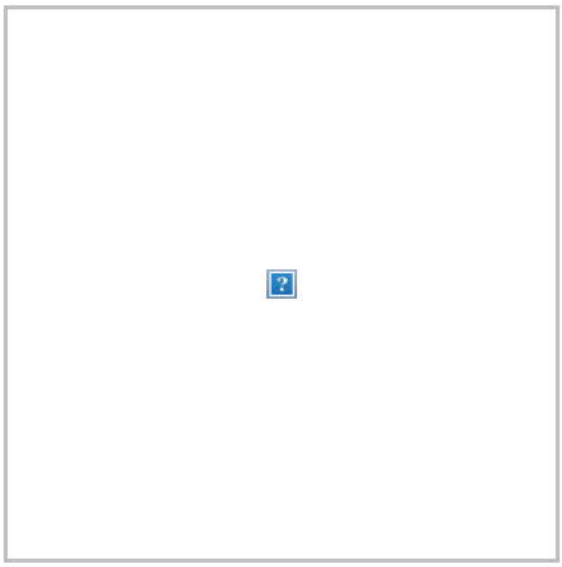
One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

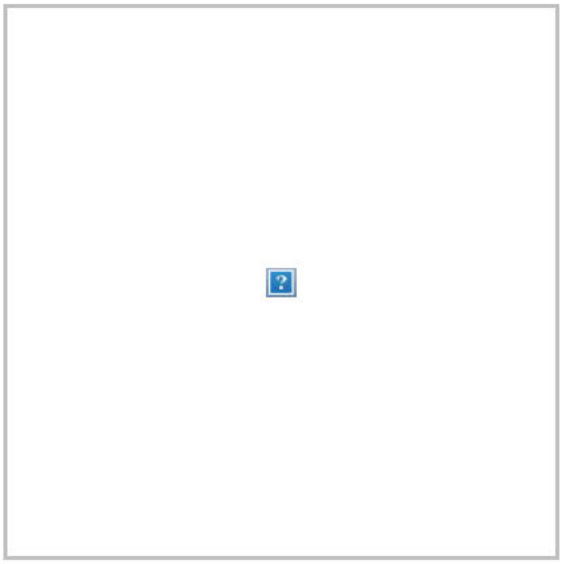
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...

NEW PRODUCTS



Flock Safety Raven

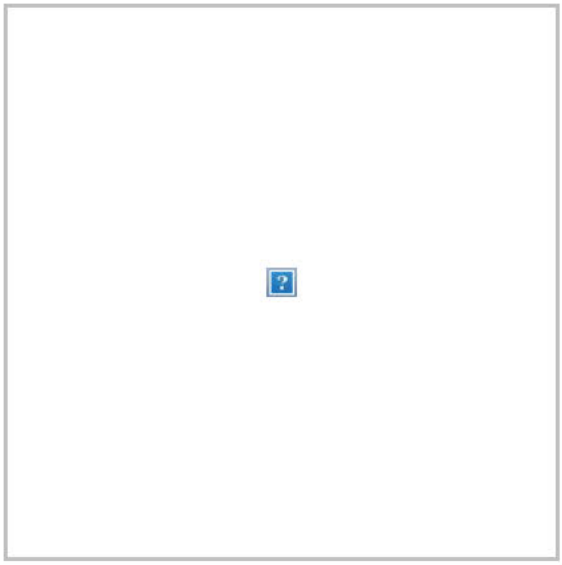
The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem



Setina Rear Cargo Storage Box

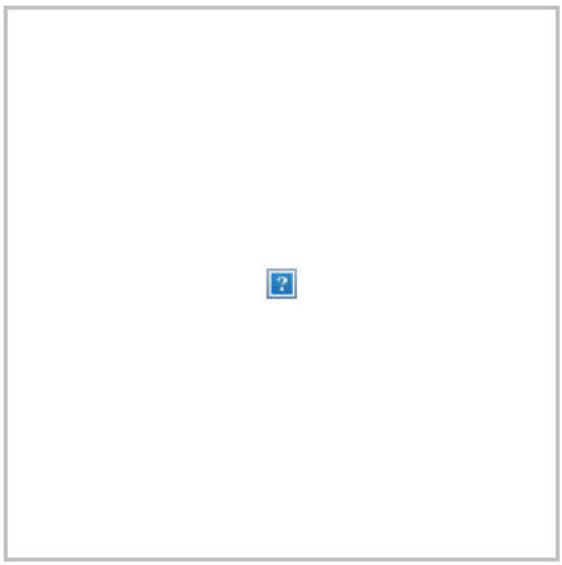
Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

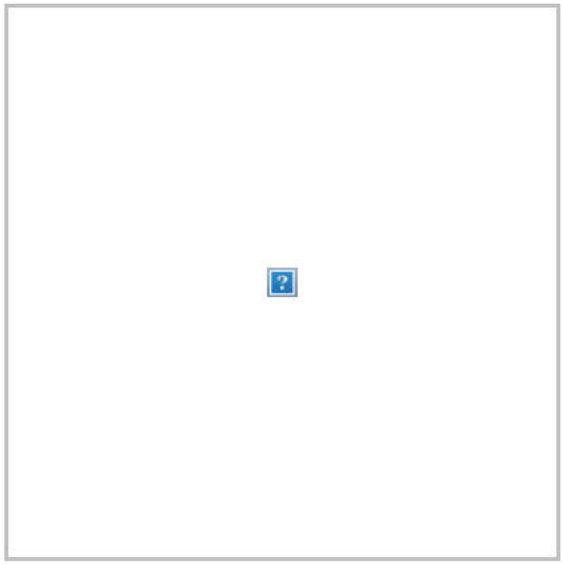


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



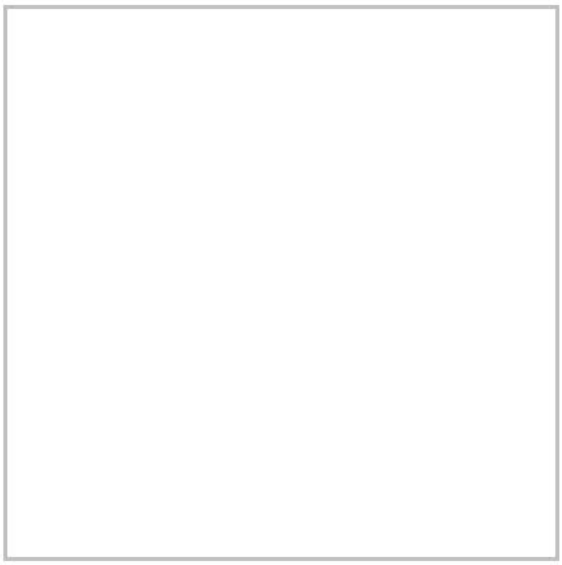
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

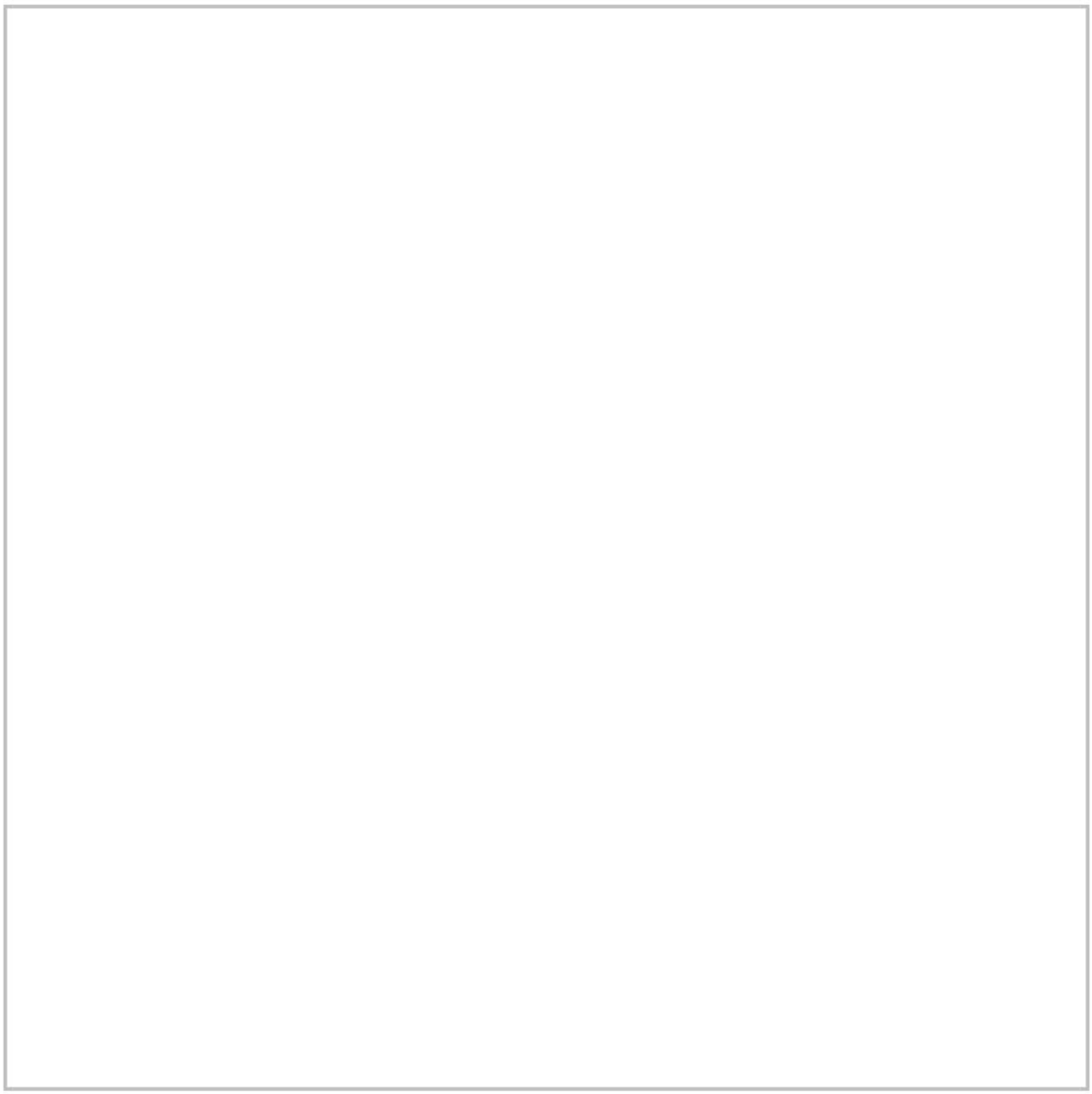
The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE



Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.

Let's Talk Holsters

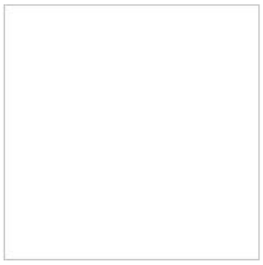
When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

2023 Uniform Trends

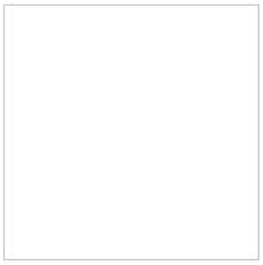
What law enforcement agencies are buying and what new products to watch.

Integrating Technology: Juggling Public Safety Mission with High-Tech

Going Digital: Harnessing Digital Forensics Technology

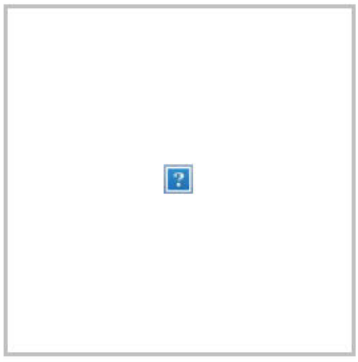


The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.



As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION



Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us



This email is being sent to edward.blackwell@pol.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: Hickey, Matthew (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:08:28 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.

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

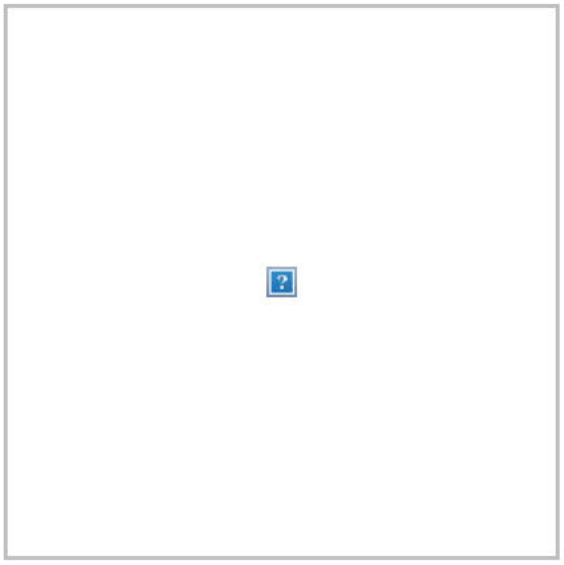
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

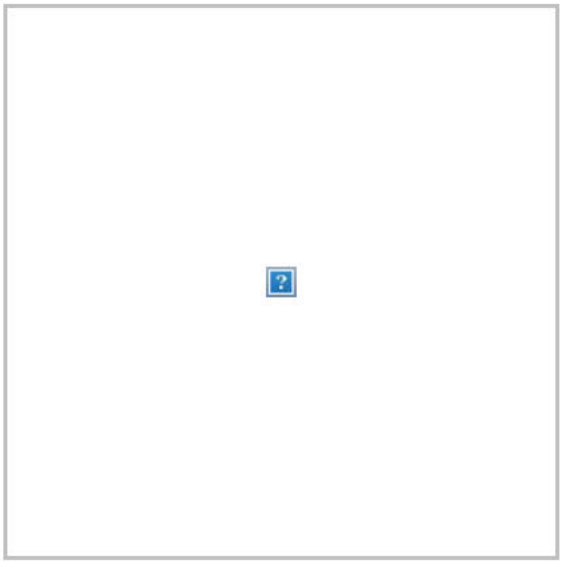
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



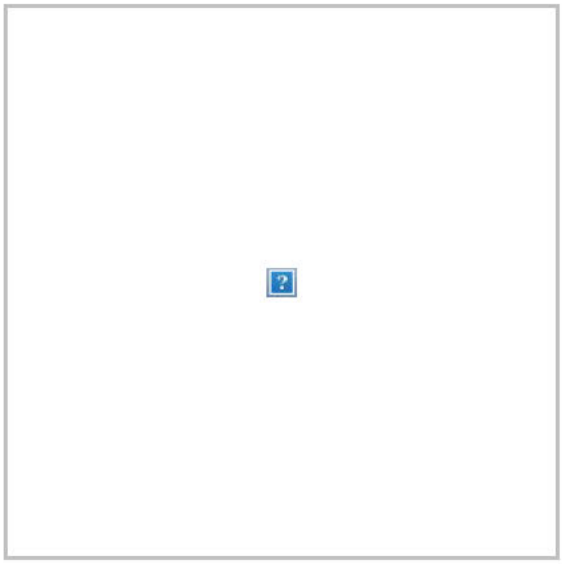
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



V-VICTA

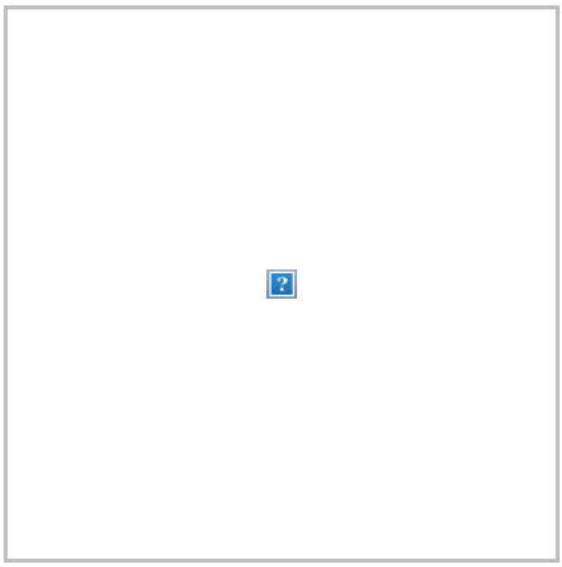
One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

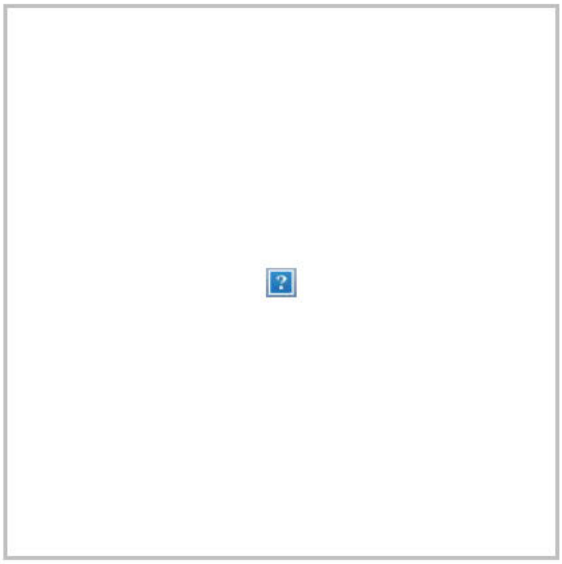
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...

NEW PRODUCTS



Flock Safety Raven

The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem

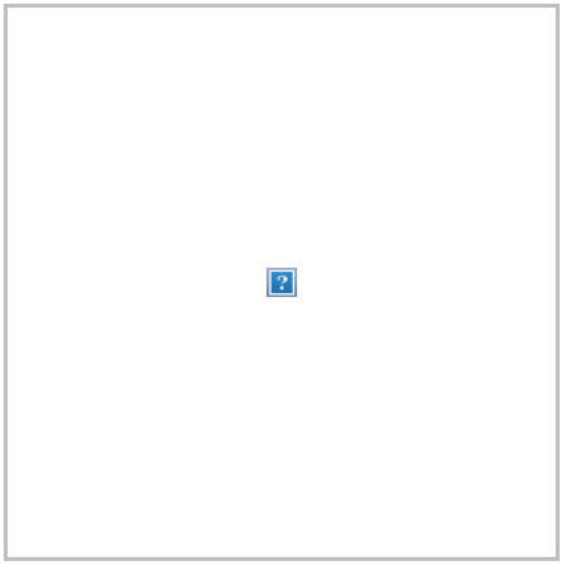


Setina Rear Cargo Storage Box

Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

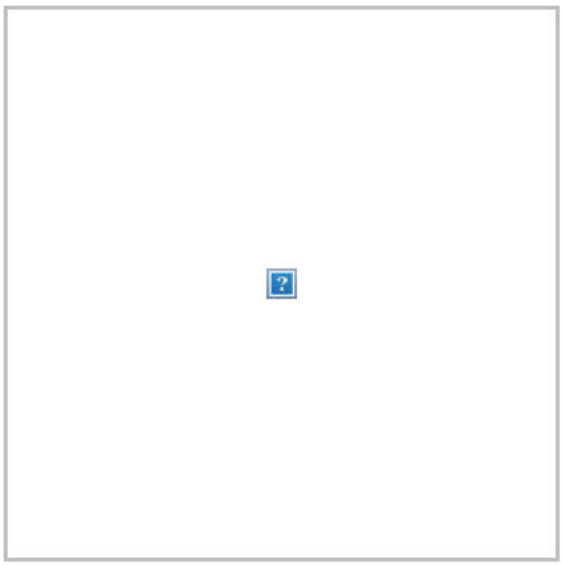


with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

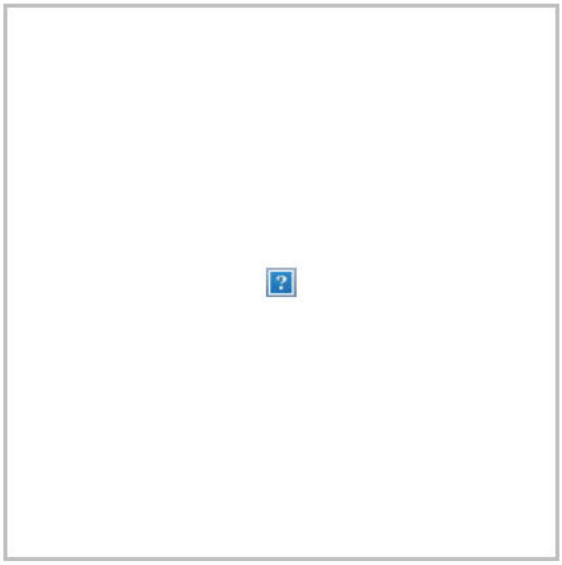


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



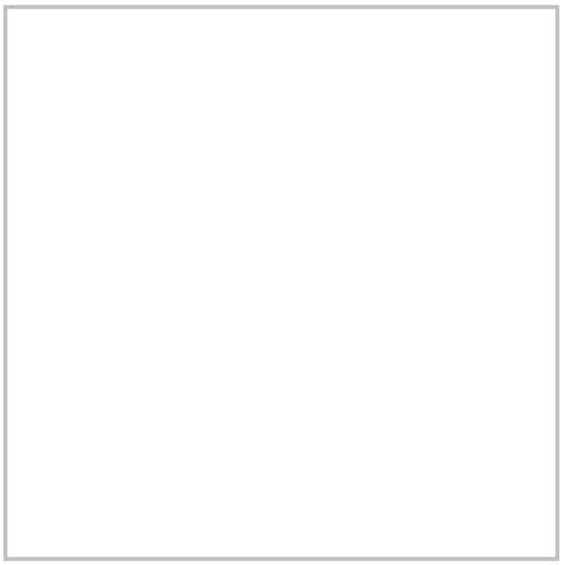
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

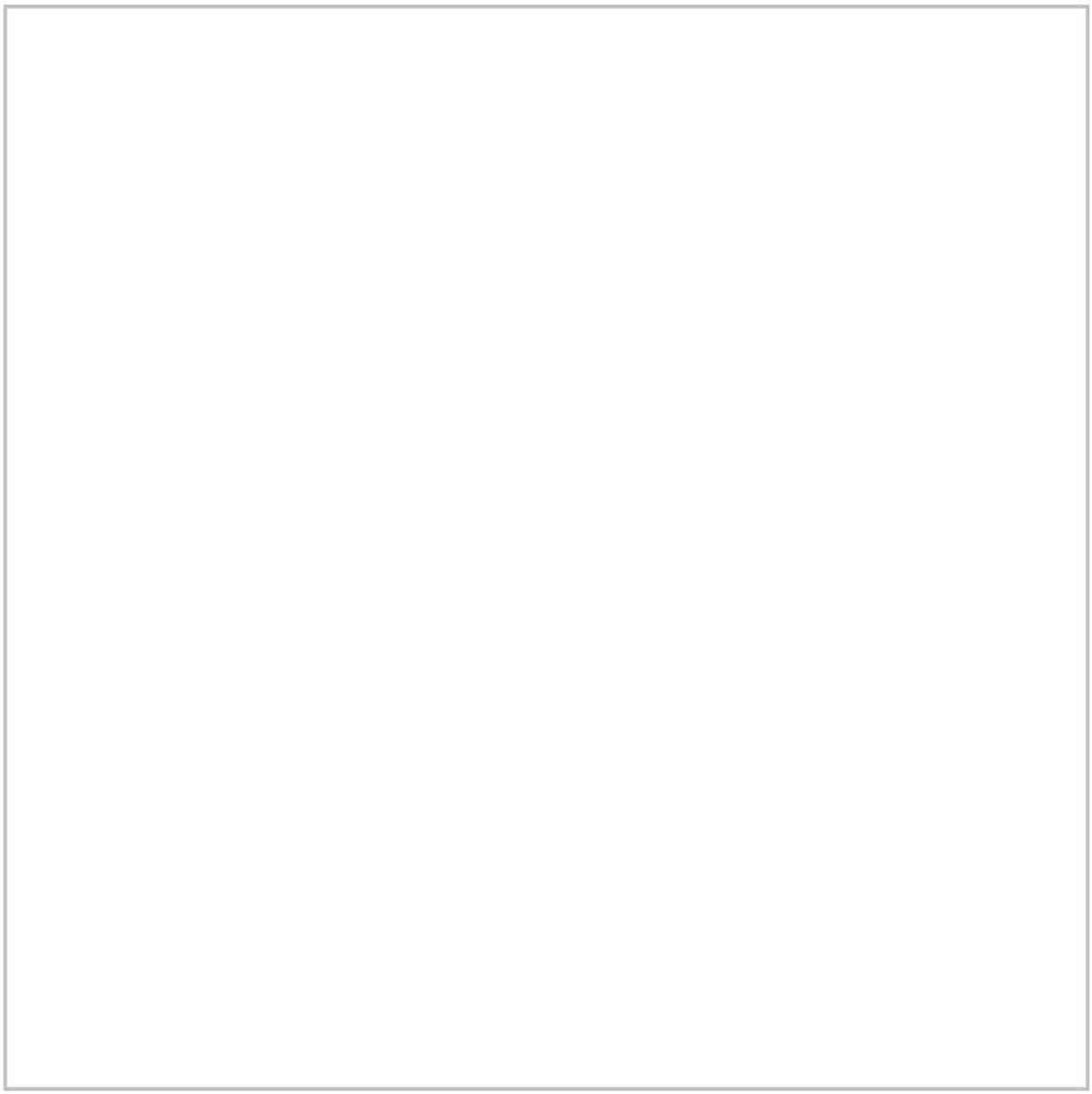
The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE



Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.

Let's Talk Holsters

When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

2023 Uniform Trends

What law enforcement agencies are buying and what new products to watch.

Integrating Technology: Juggling Public Safety Mission with High-Tech

Going Digital: Harnessing Digital Forensics Technology

The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.

As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION

Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us

This email is being sent to matthew.hickey@pol.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: Dear, Anthony (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:08:18 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.

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

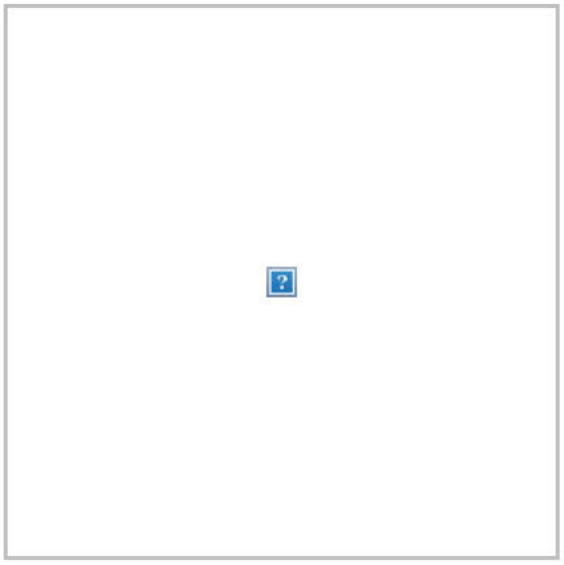
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

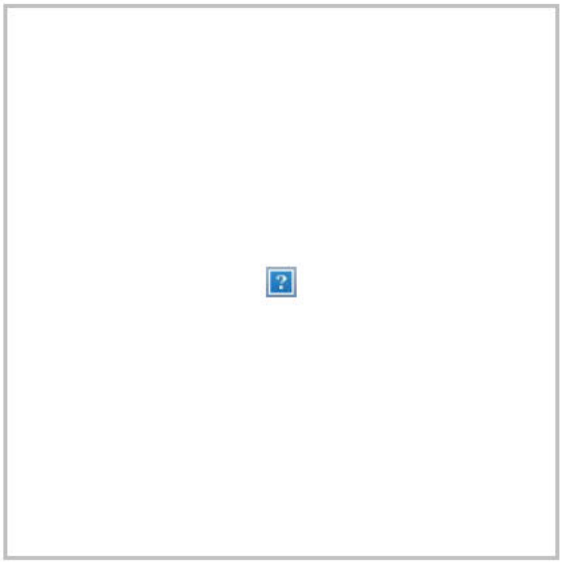
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



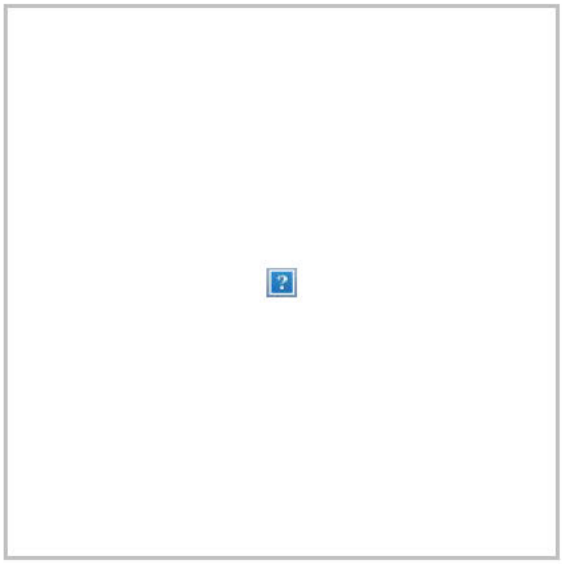
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



V-VICTA

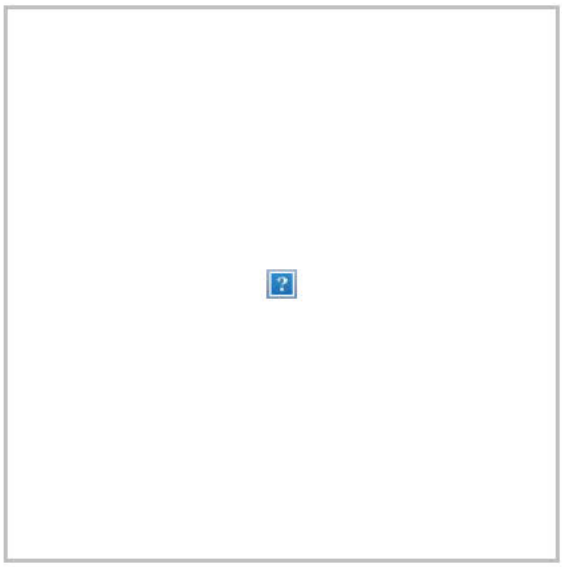
One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

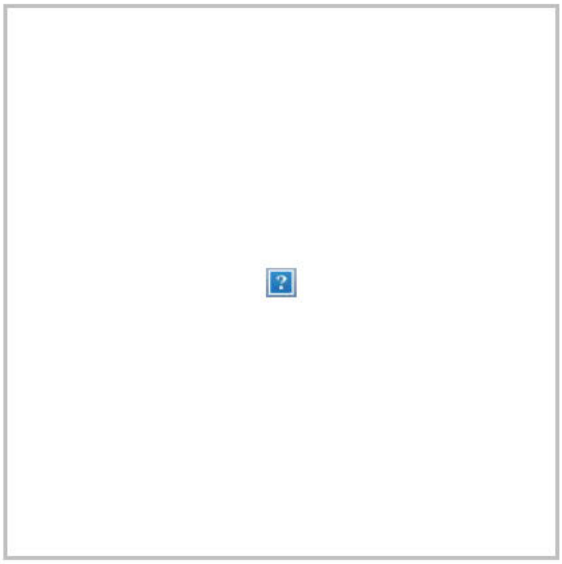
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...

NEW PRODUCTS



Flock Safety Raven

The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem

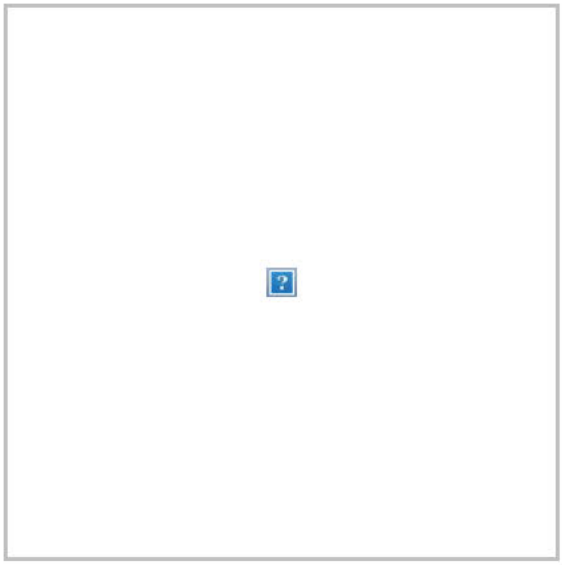


Setina Rear Cargo Storage Box

Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

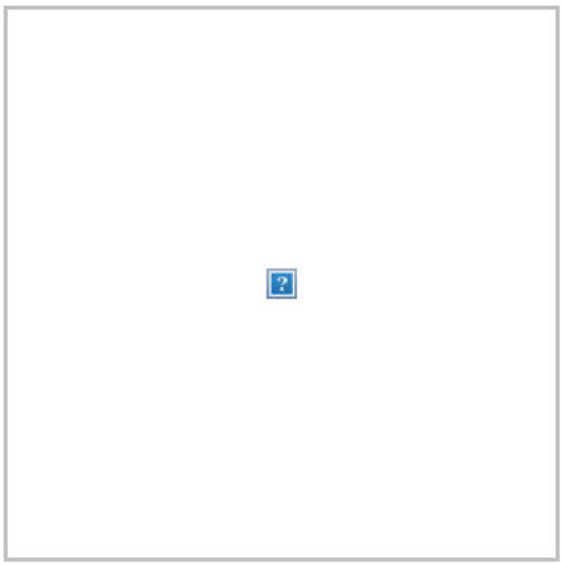


with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

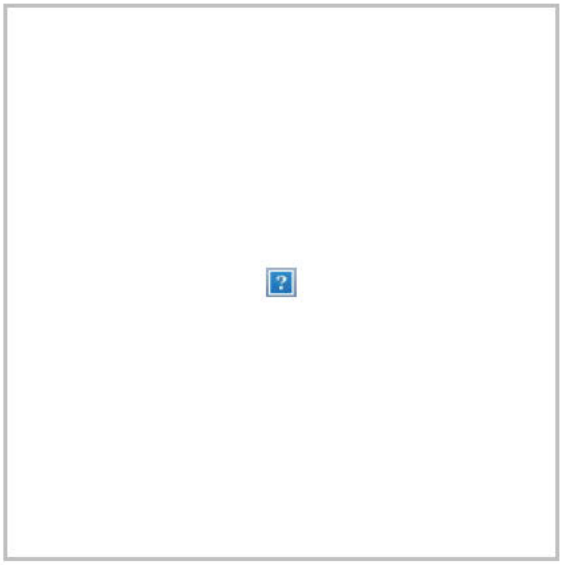


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



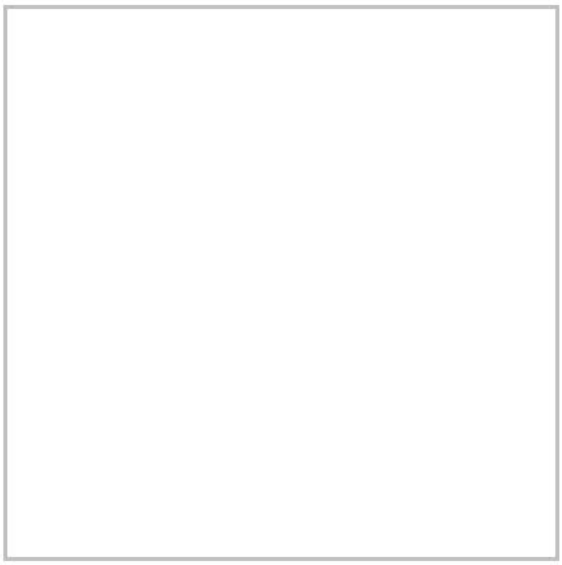
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

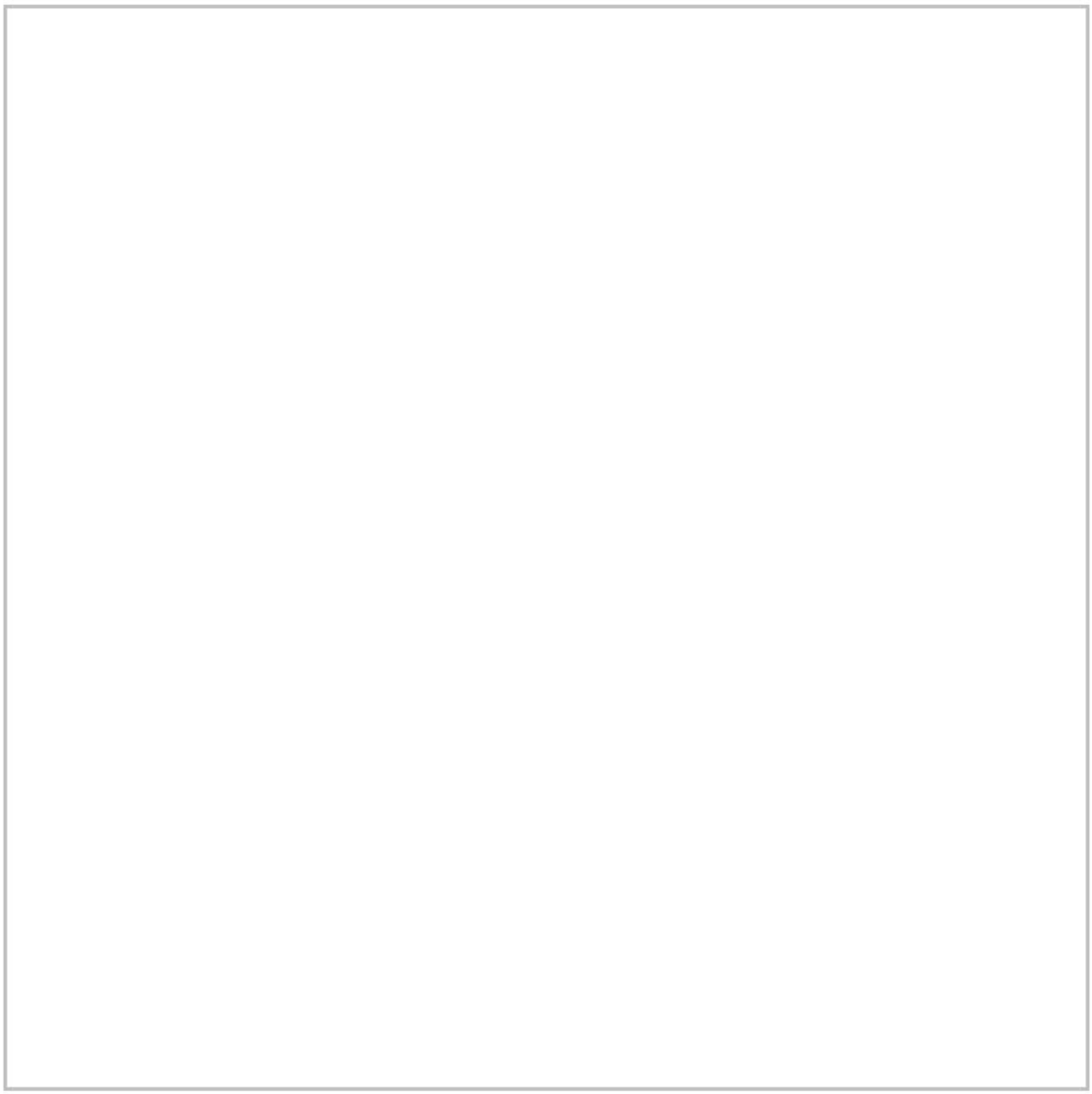
The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE



Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.



Let's Talk Holsters

When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

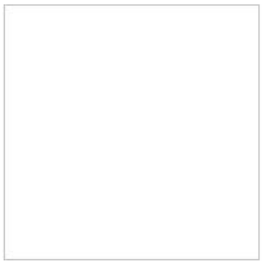
Integrating Technology: Juggling Public Safety Mission with High-Tech



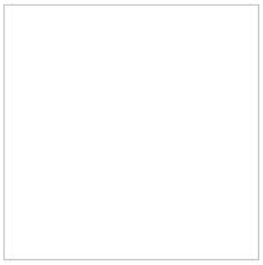
2023 Uniform Trends

What law enforcement agencies are buying and what new products to watch.

Going Digital: Harnessing Digital Forensics Technology

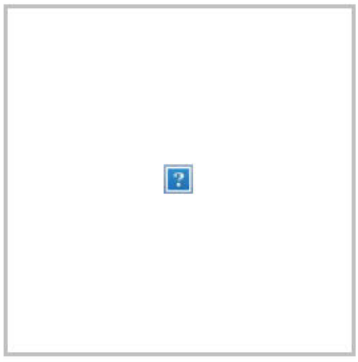


The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.



As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION



Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us



This email is being sent to anthony.dear@pol.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: Ditata, Matthew (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:08:10 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.

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

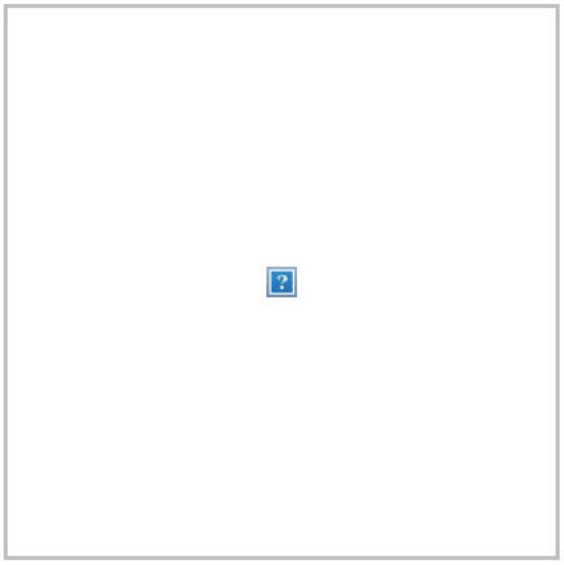
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

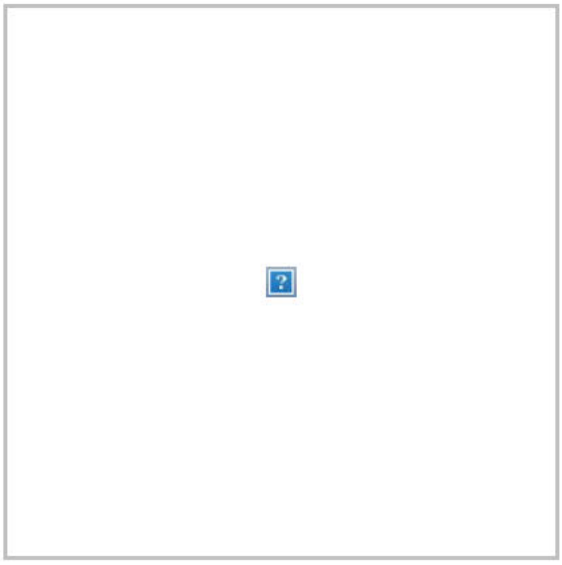
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



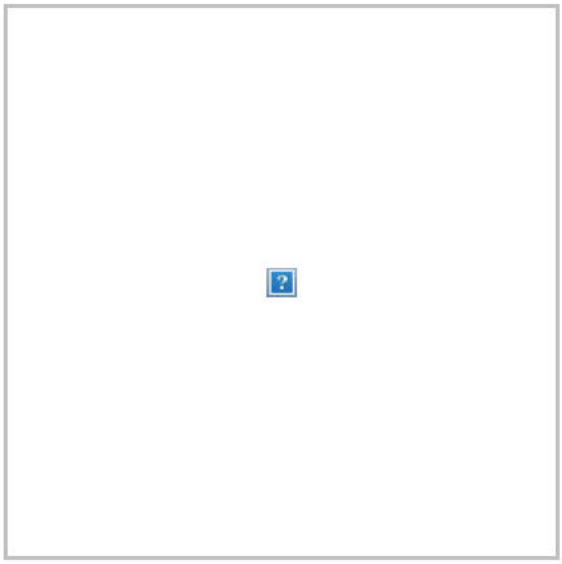
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



V-VICTA

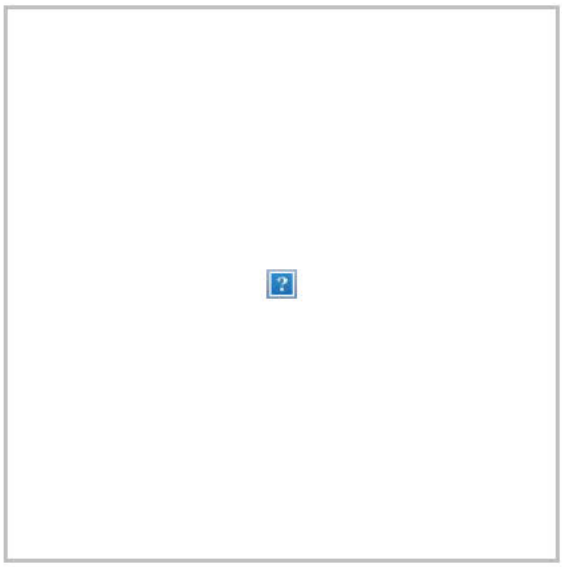
One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

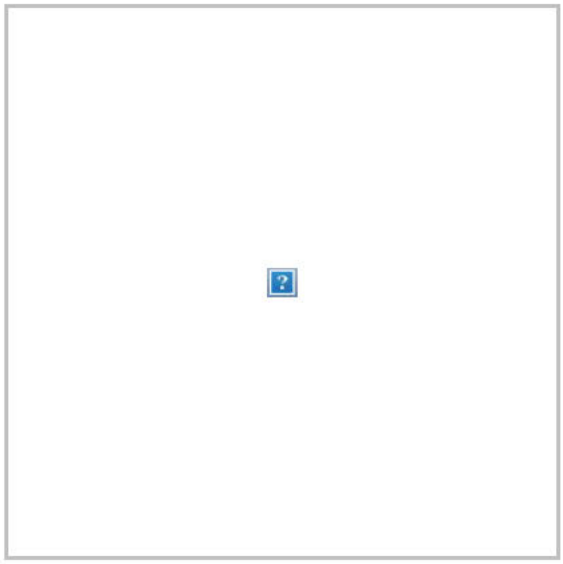
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...

NEW PRODUCTS



Flock Safety Raven

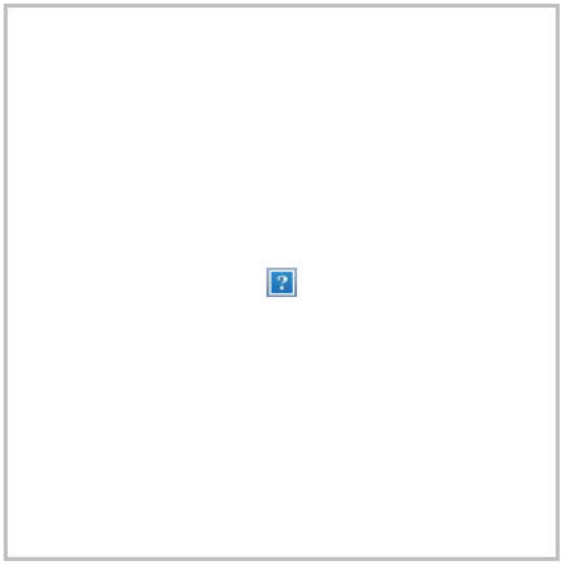
The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem



Setina Rear Cargo Storage Box

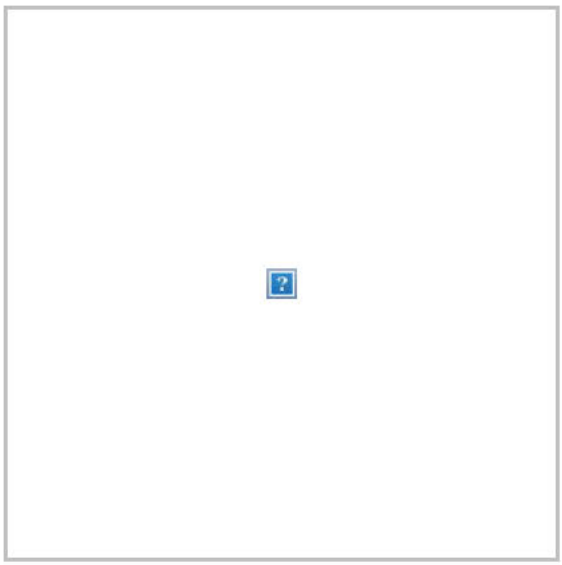
Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

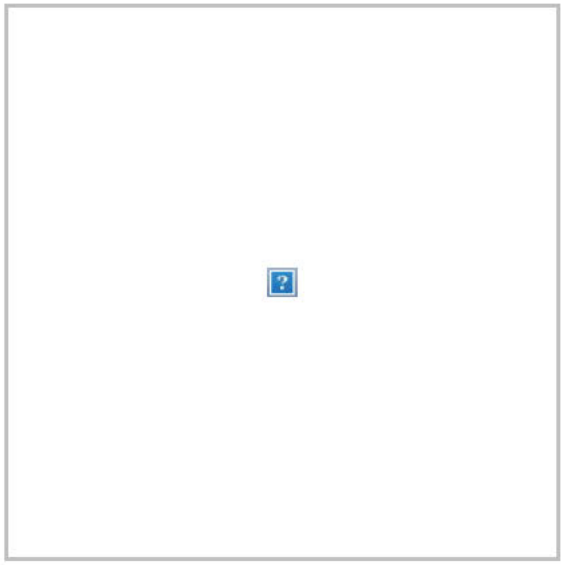


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



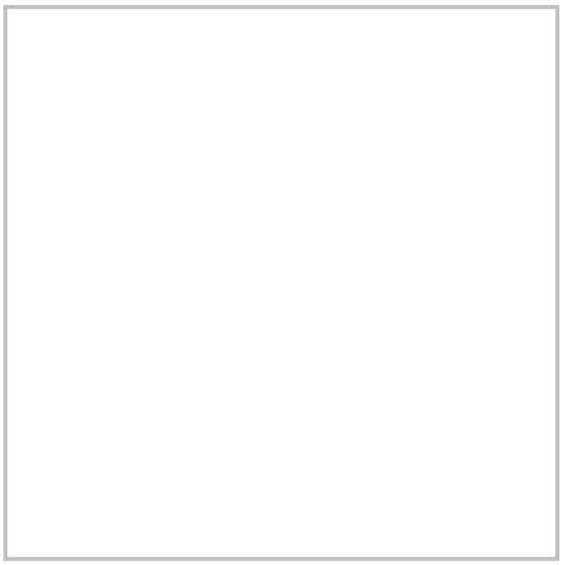
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

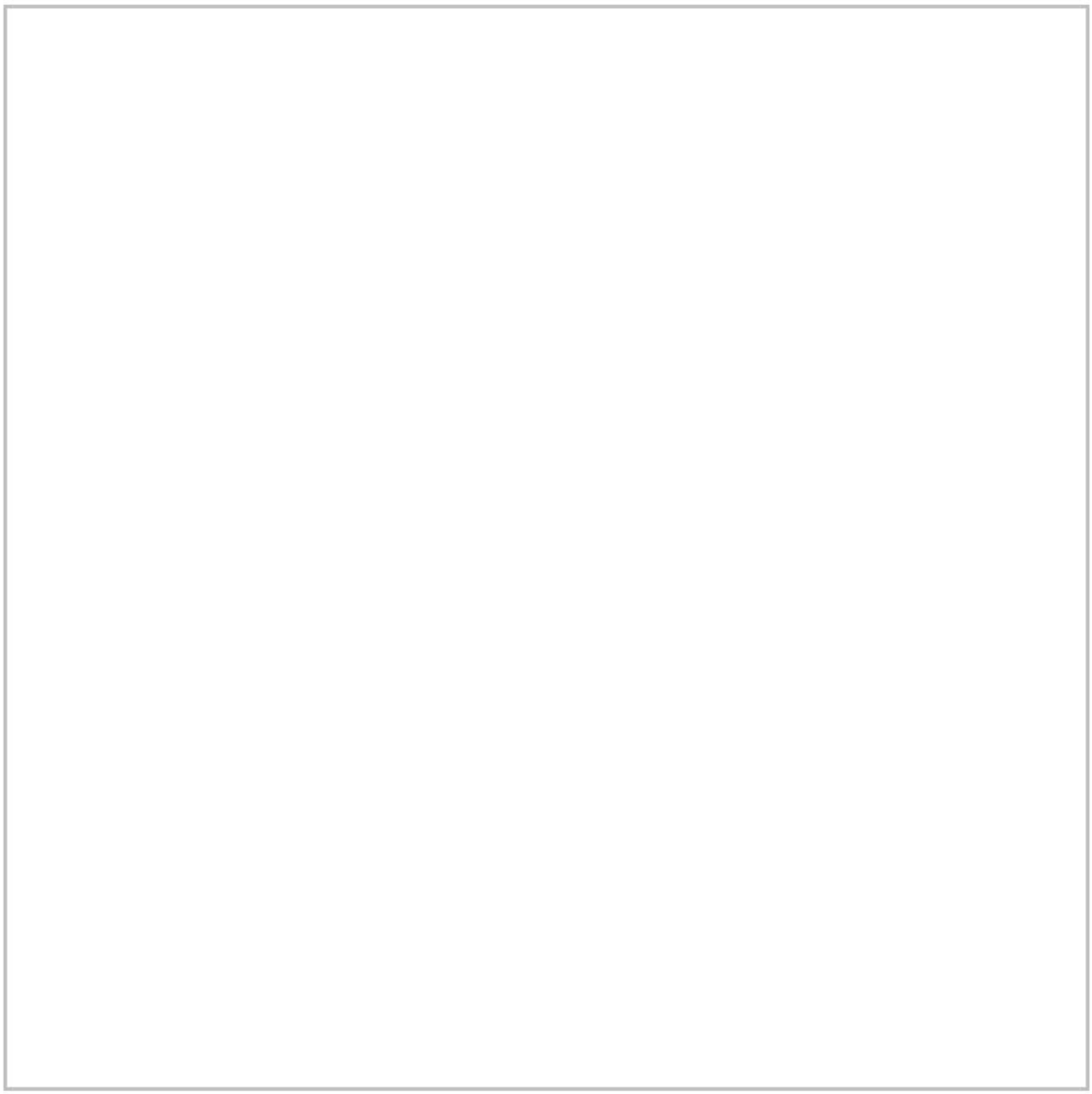
The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE



Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.



Let's Talk Holsters

When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

Integrating Technology: Juggling Public Safety Mission with High-Tech



2023 Uniform Trends

What law enforcement agencies are buying and what new products to watch.

Going Digital: Harnessing Digital Forensics Technology

The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.

As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION

Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us

This email is being sent to matthew.ditata@pol.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: zzHuber, Richard (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:08:08 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.

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

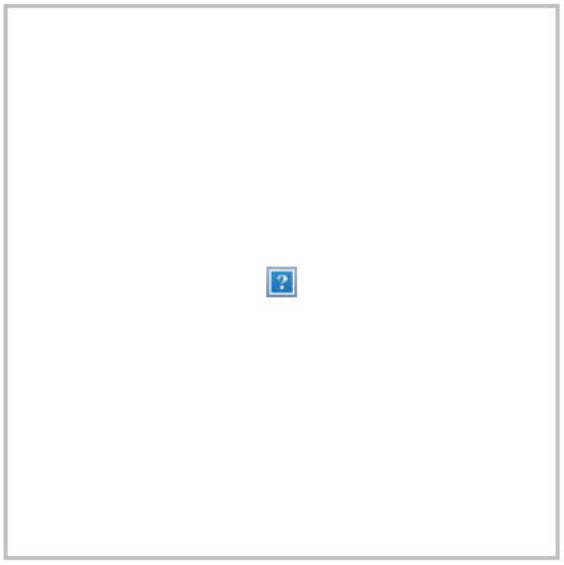
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

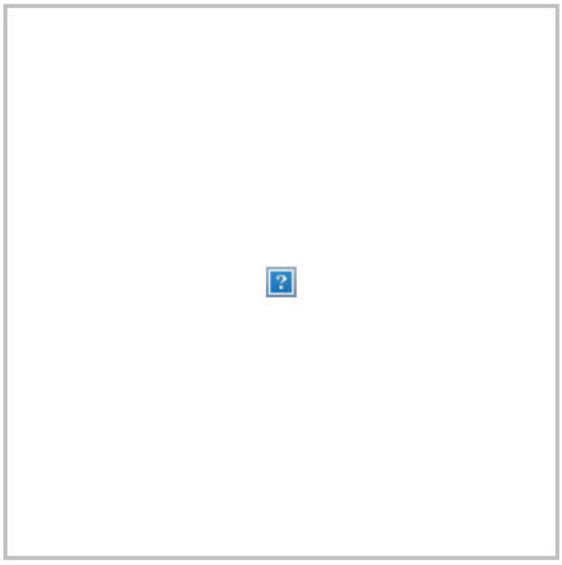
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



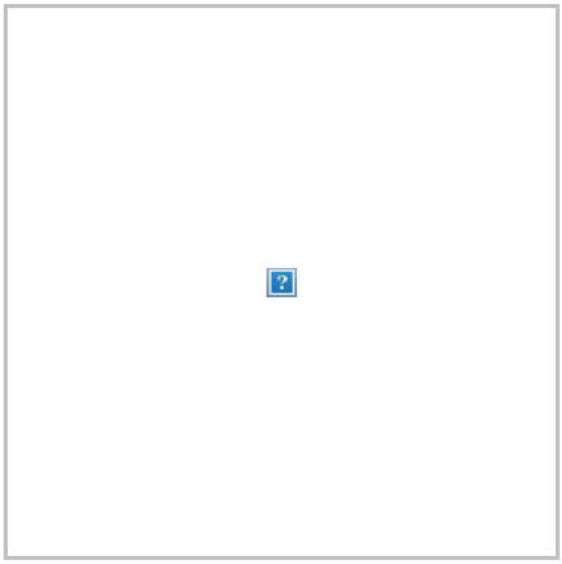
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



V-VICTA

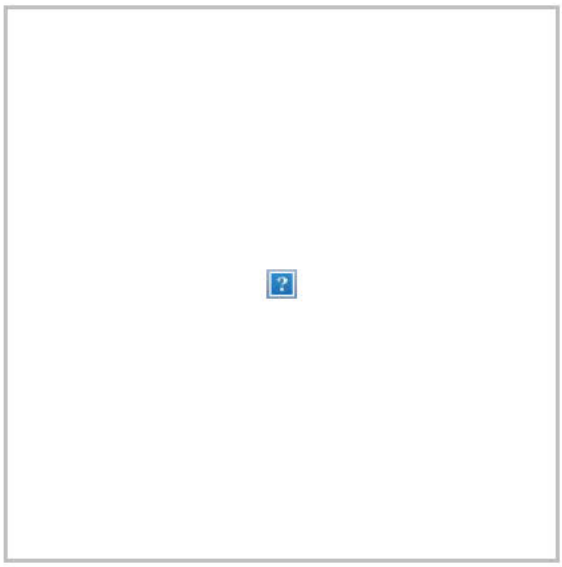
One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

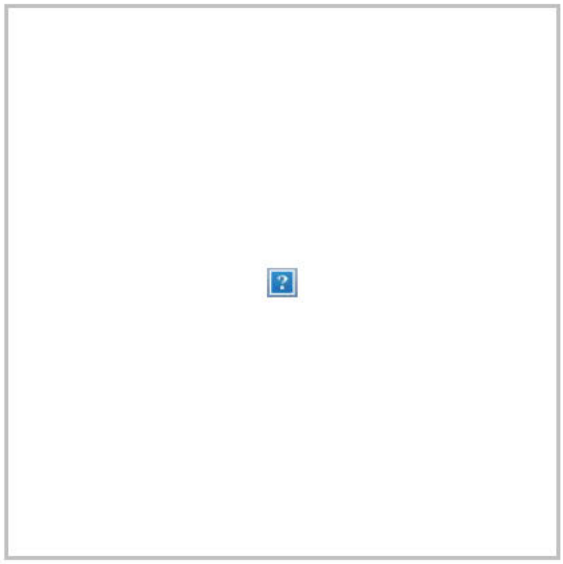
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...

NEW PRODUCTS



Flock Safety Raven

The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem

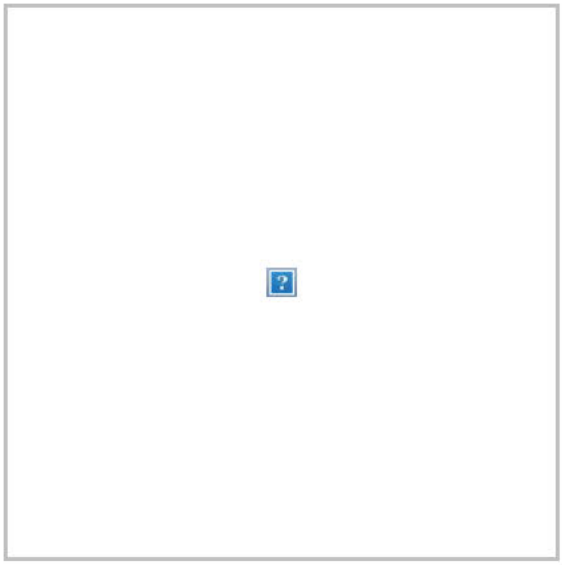


Setina Rear Cargo Storage Box

Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

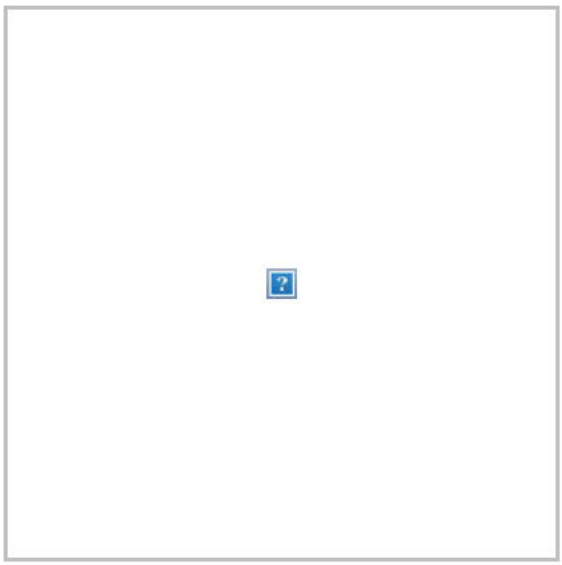


with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

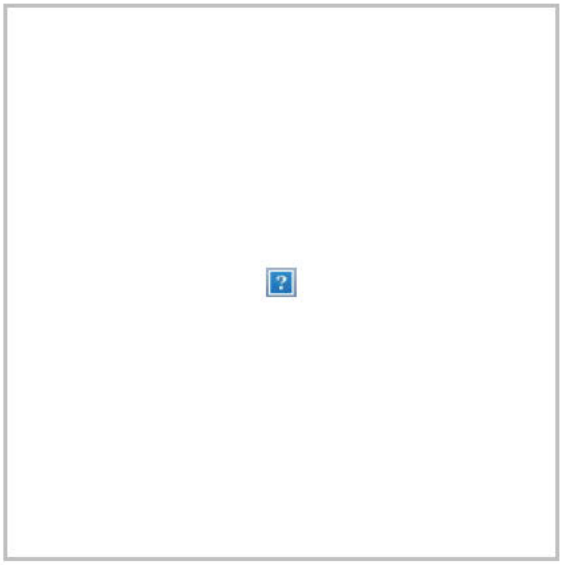


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



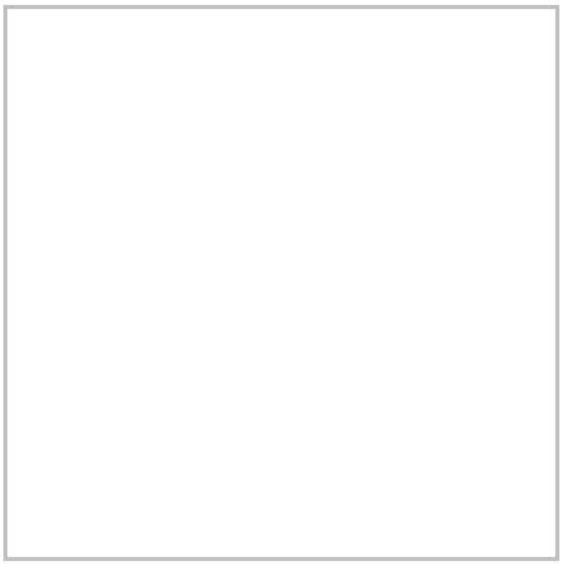
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE

Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.

Let's Talk Holsters

When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

2023 Uniform Trends

What law enforcement agencies are buying and what new products to watch.

Integrating Technology: Juggling Public Safety Mission with High-Tech

Going Digital: Harnessing Digital Forensics Technology

The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.

As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION

Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us

This email is being sent to richard.huber@pol.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: zzMoran, John (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:07:50 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.

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

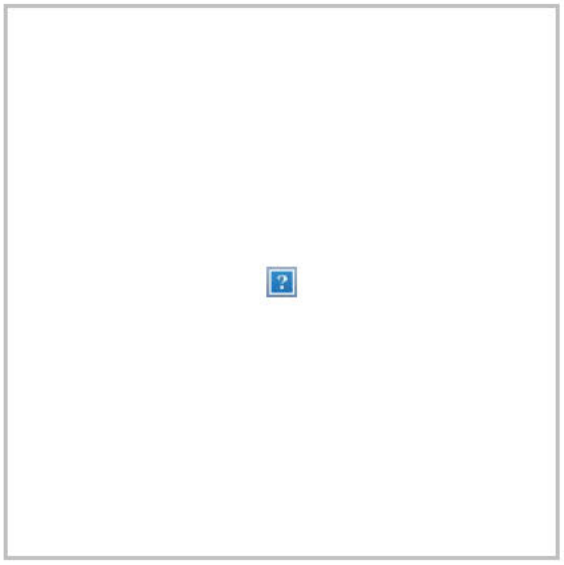
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

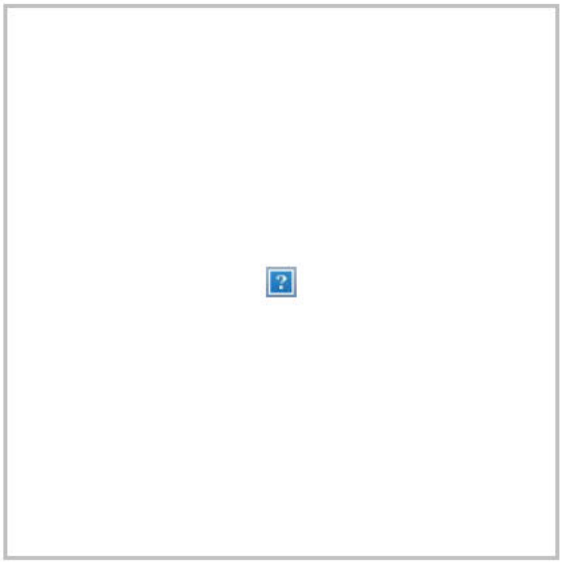
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



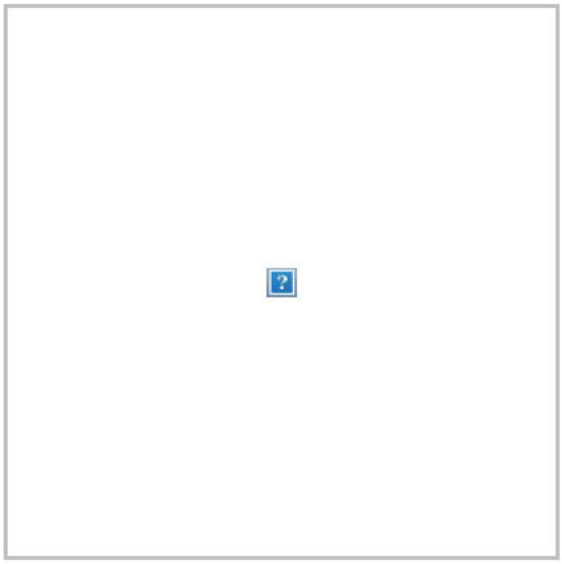
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



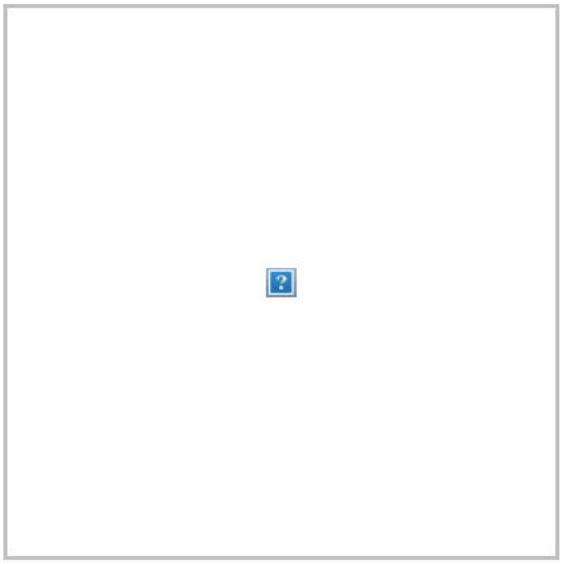
V-VICTA

One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

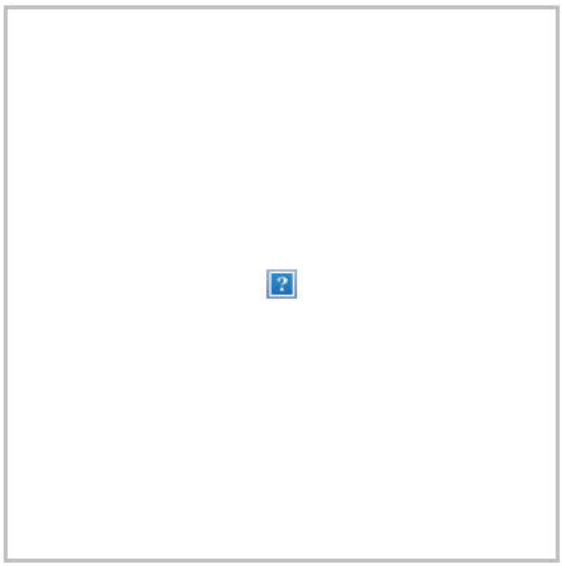
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...



Setina Rear Cargo Storage Box

Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

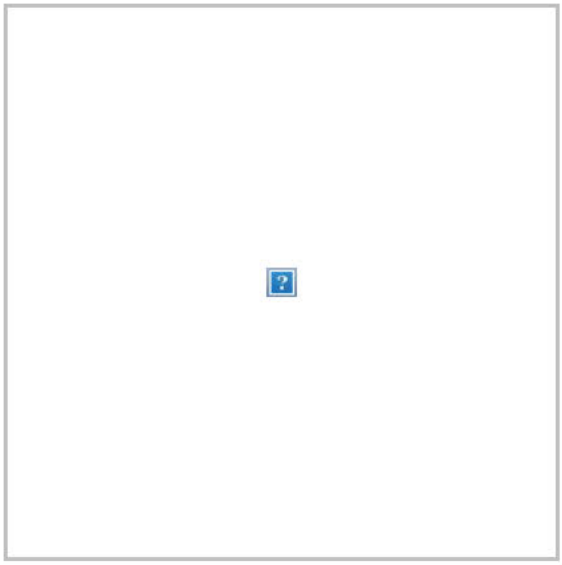
NEW PRODUCTS



Flock Safety Raven

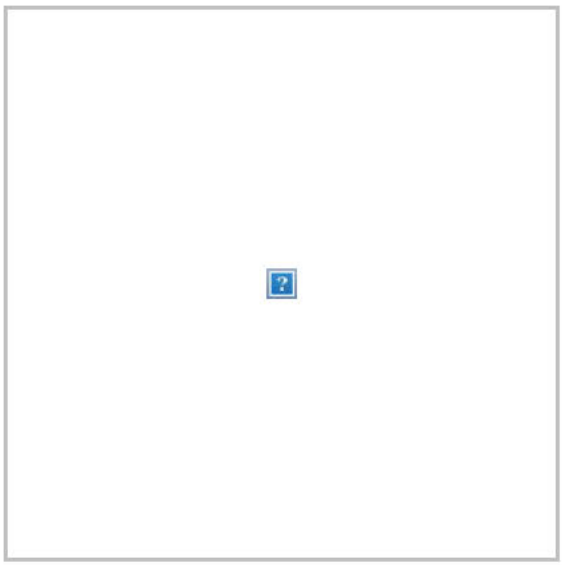
The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem

with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

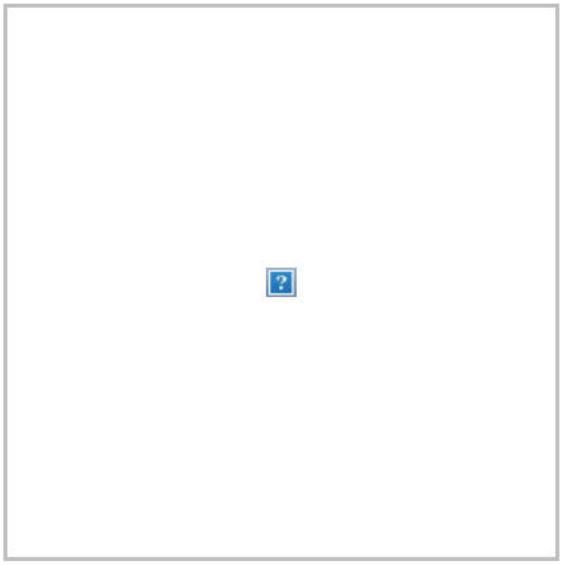


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



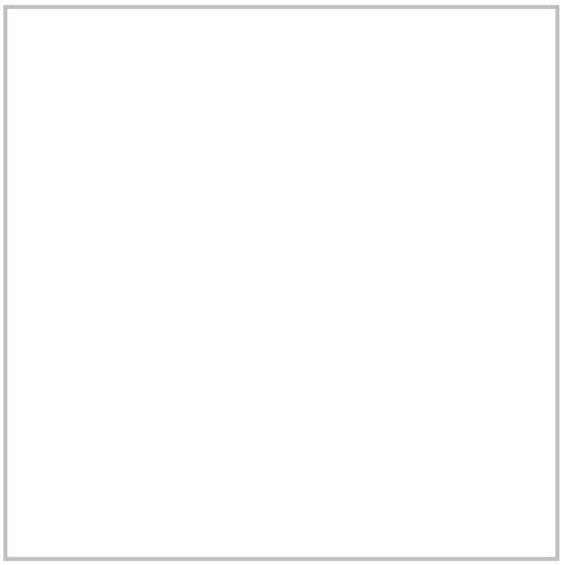
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

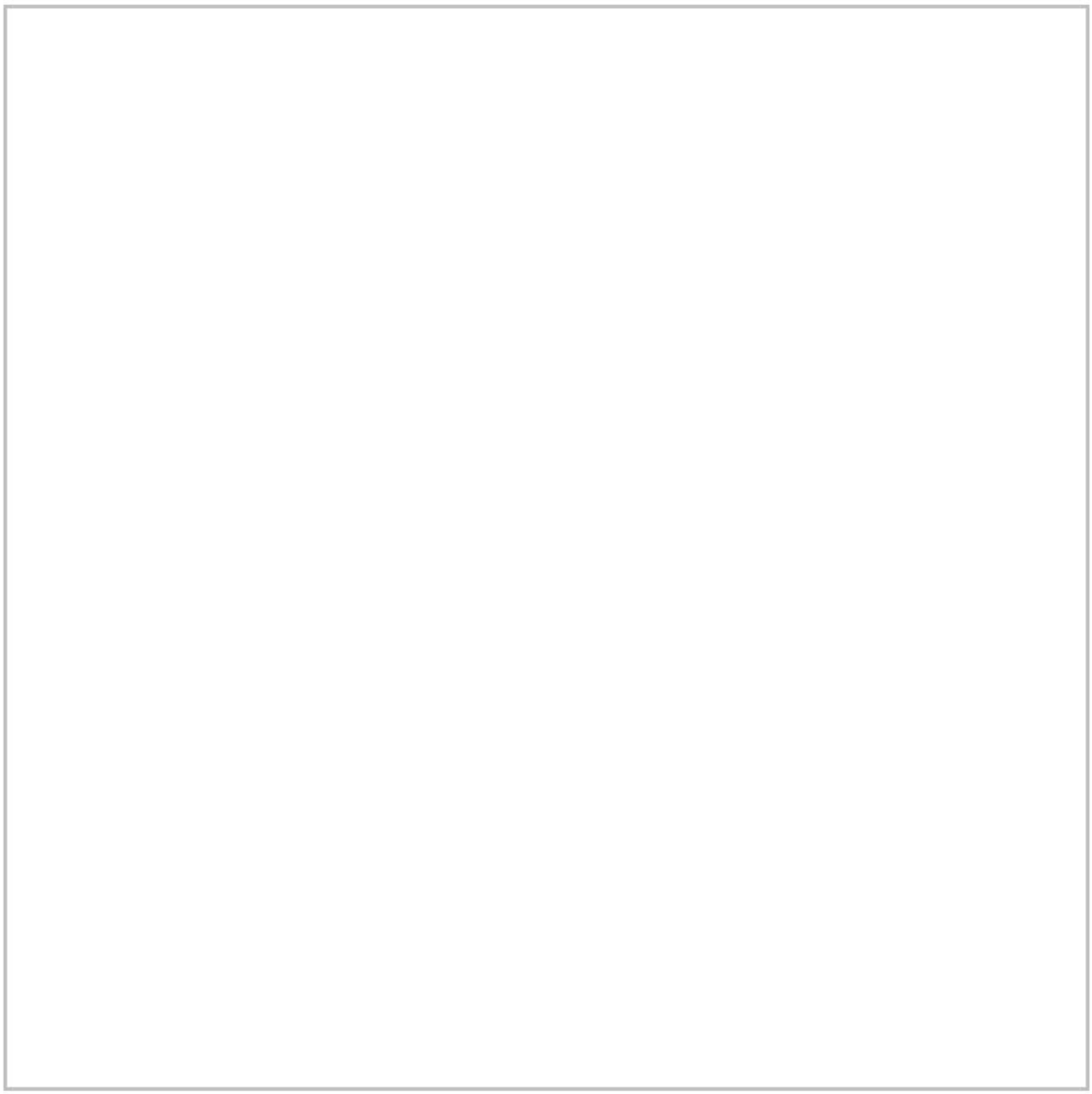
The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE



Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.

Let's Talk Holsters

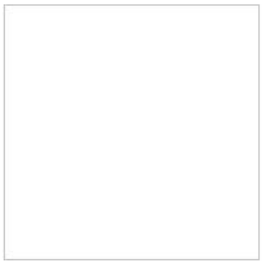
When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

2023 Uniform Trends

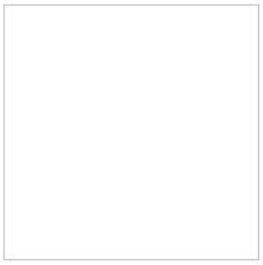
What law enforcement agencies are buying and what new products to watch.

Integrating Technology: Juggling Public Safety Mission with High-Tech

Going Digital: Harnessing Digital Forensics Technology

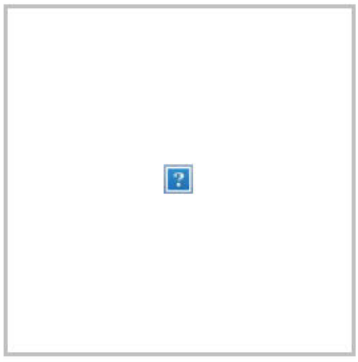


The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.



As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION



Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us



This email is being sent to john.moran@pol.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: Courtois, Mark (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:07:37 PM

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

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

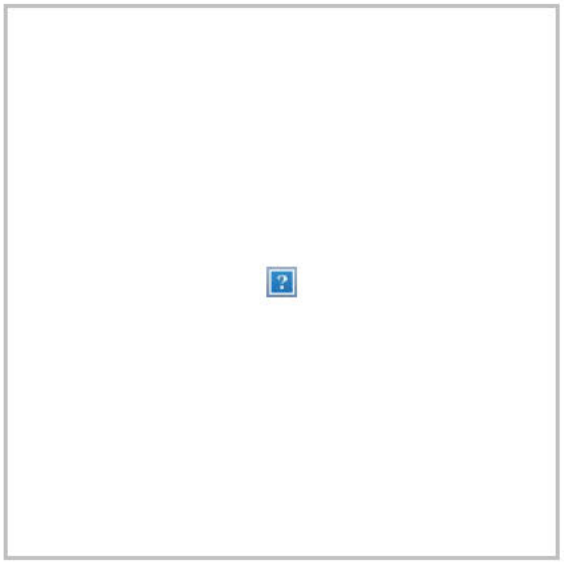
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

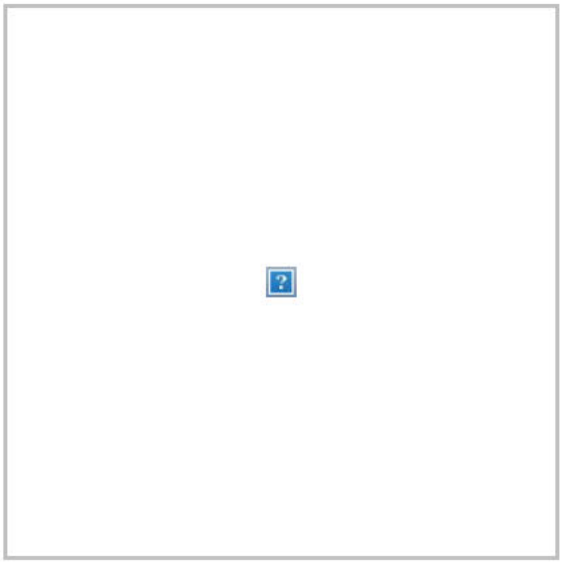
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



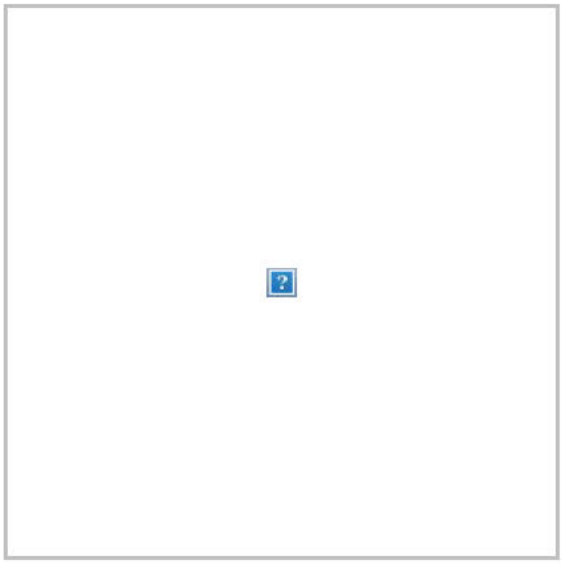
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



V-VICTA

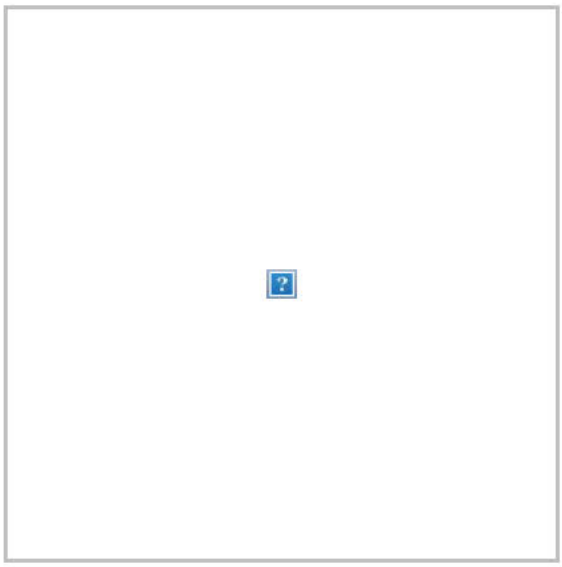
One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

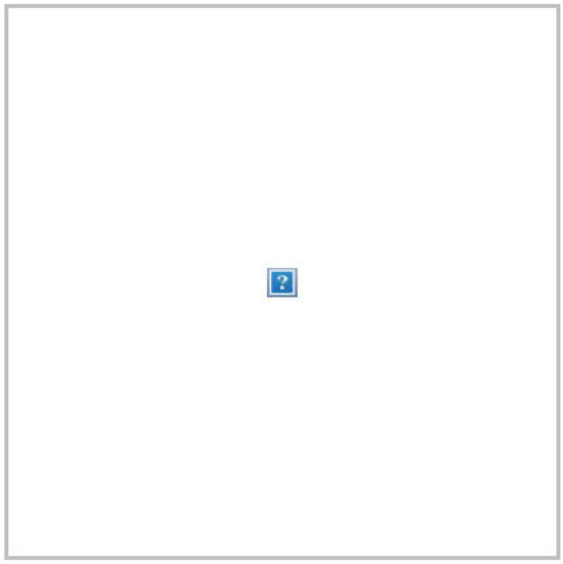
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...

NEW PRODUCTS



Flock Safety Raven

The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem

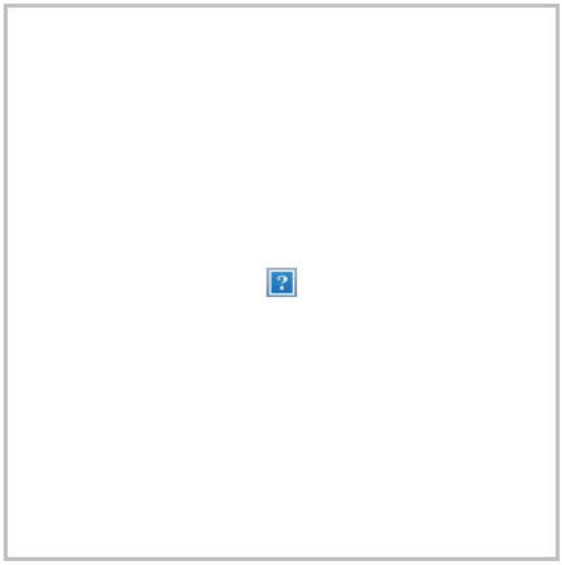


Setina Rear Cargo Storage Box

Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

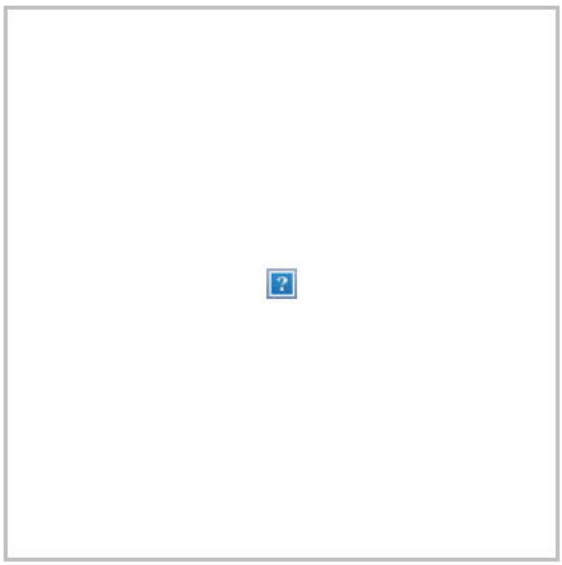


with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

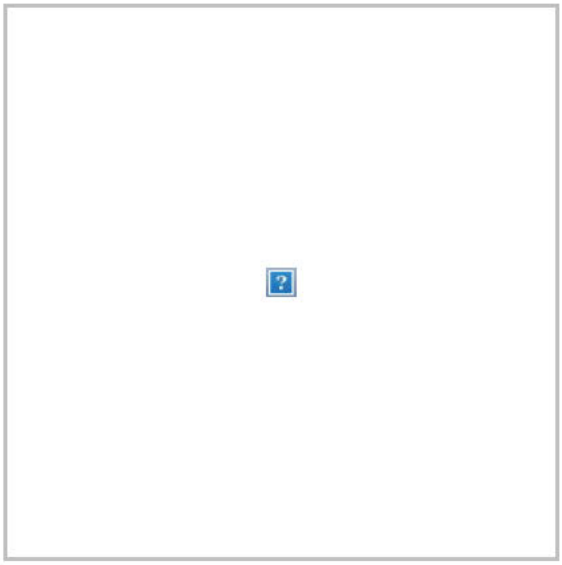


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



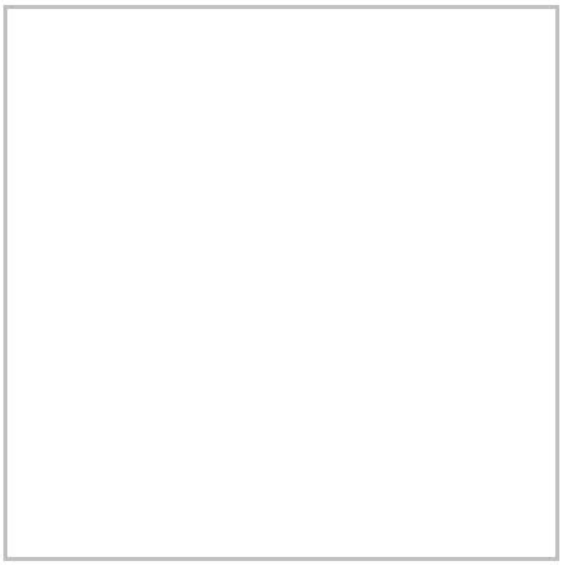
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

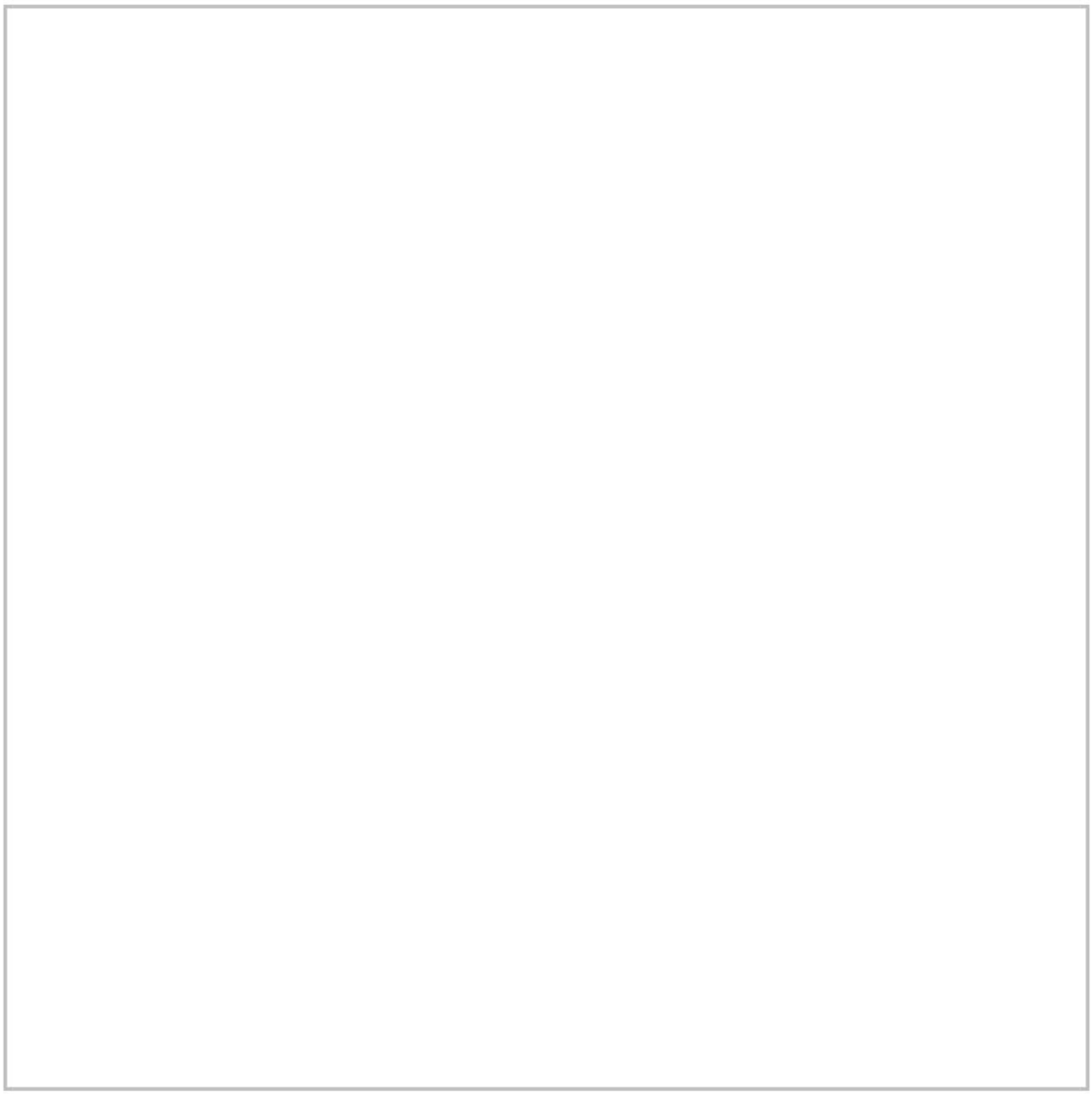
The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE



Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.



Let's Talk Holsters

When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

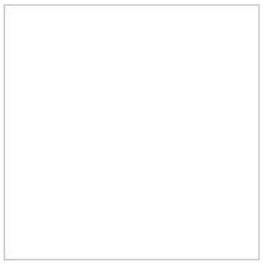
Integrating Technology: Juggling Public Safety Mission with High-Tech



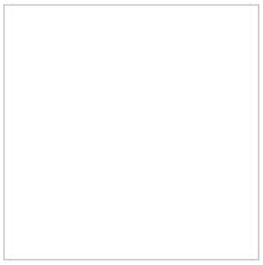
2023 Uniform Trends

What law enforcement agencies are buying and what new products to watch.

Going Digital: Harnessing Digital Forensics Technology

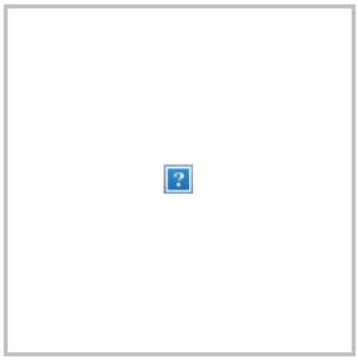


The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.



As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION



Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us



This email is being sent to mark.courtois@massmail.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: zzGenduso, Leigha (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:07:29 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.

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

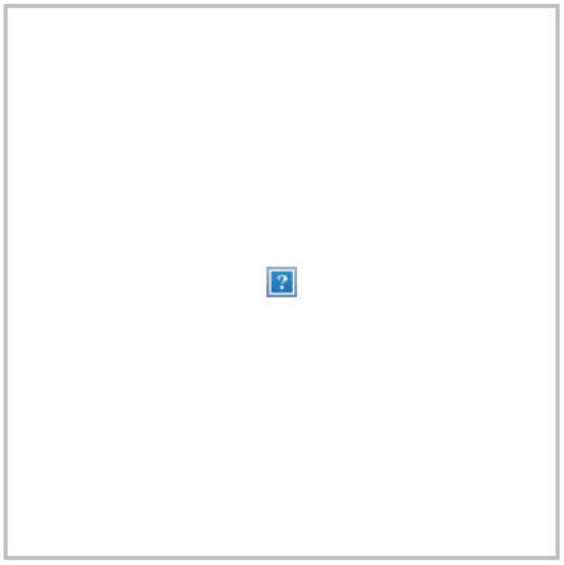
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

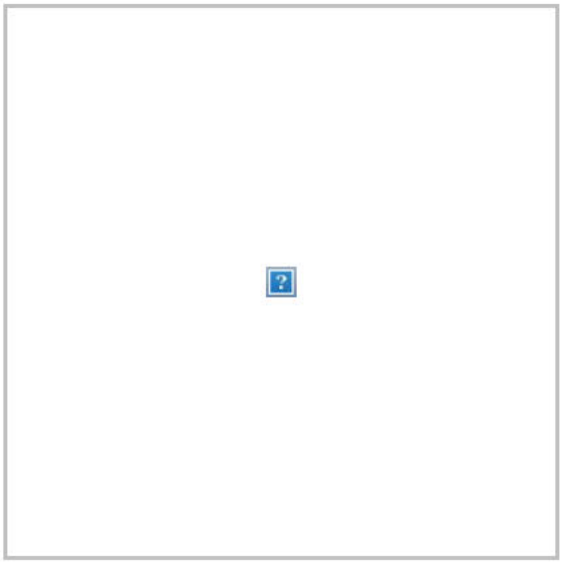
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



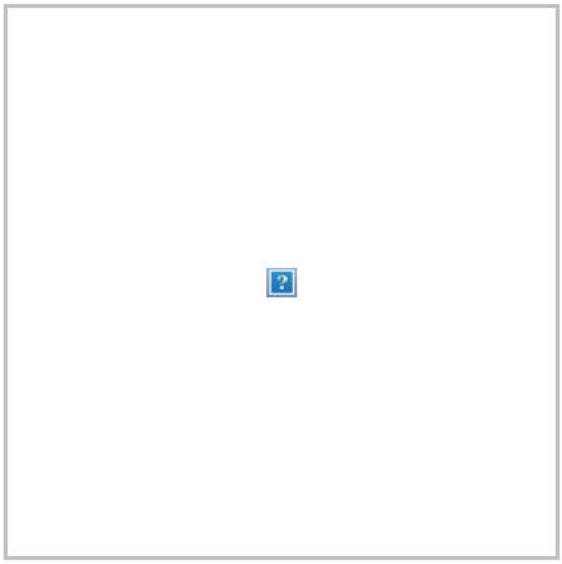
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



V-VICTA

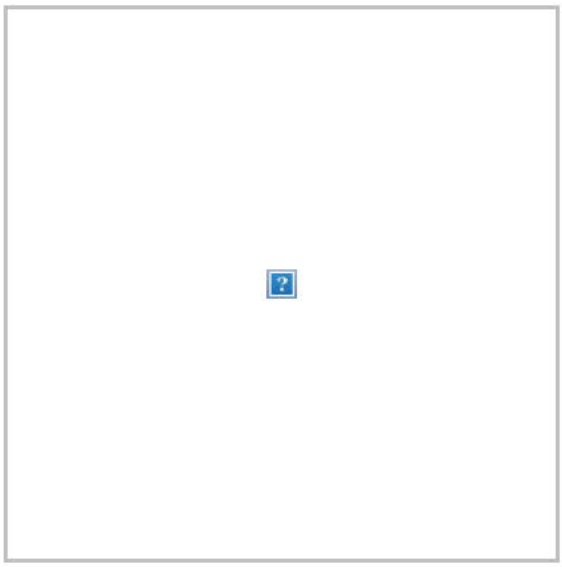
One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

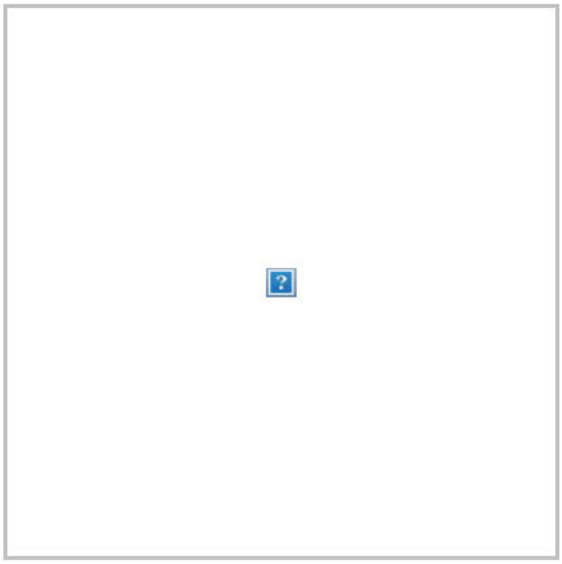
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...

NEW PRODUCTS



Flock Safety Raven

The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem

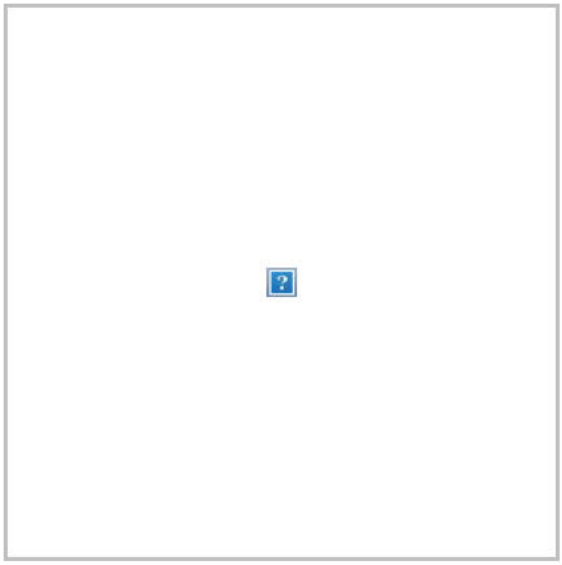


Setina Rear Cargo Storage Box

Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

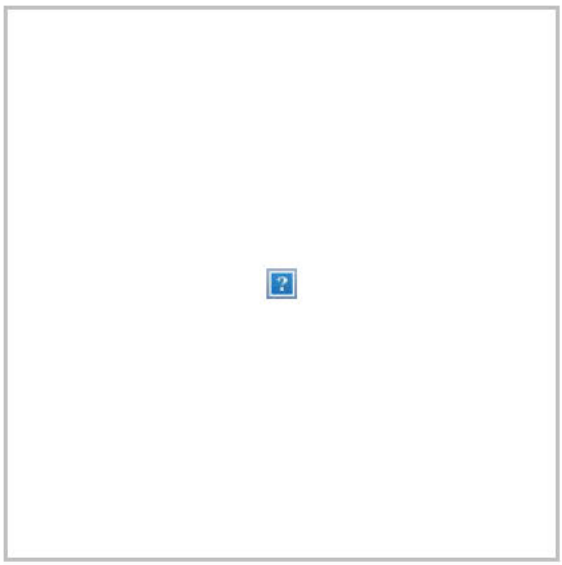


with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

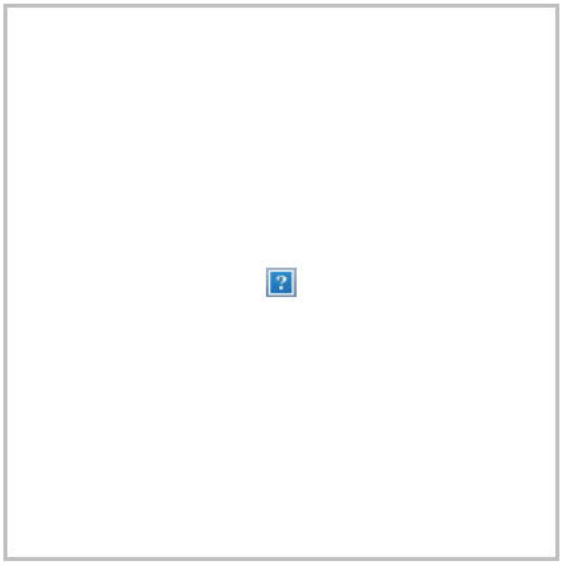


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



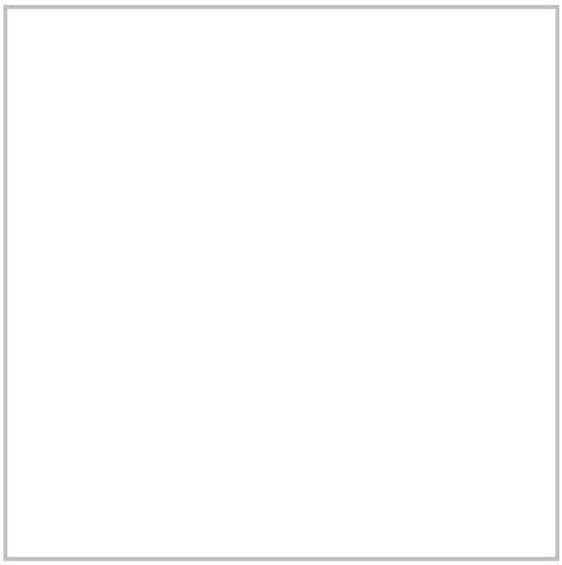
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

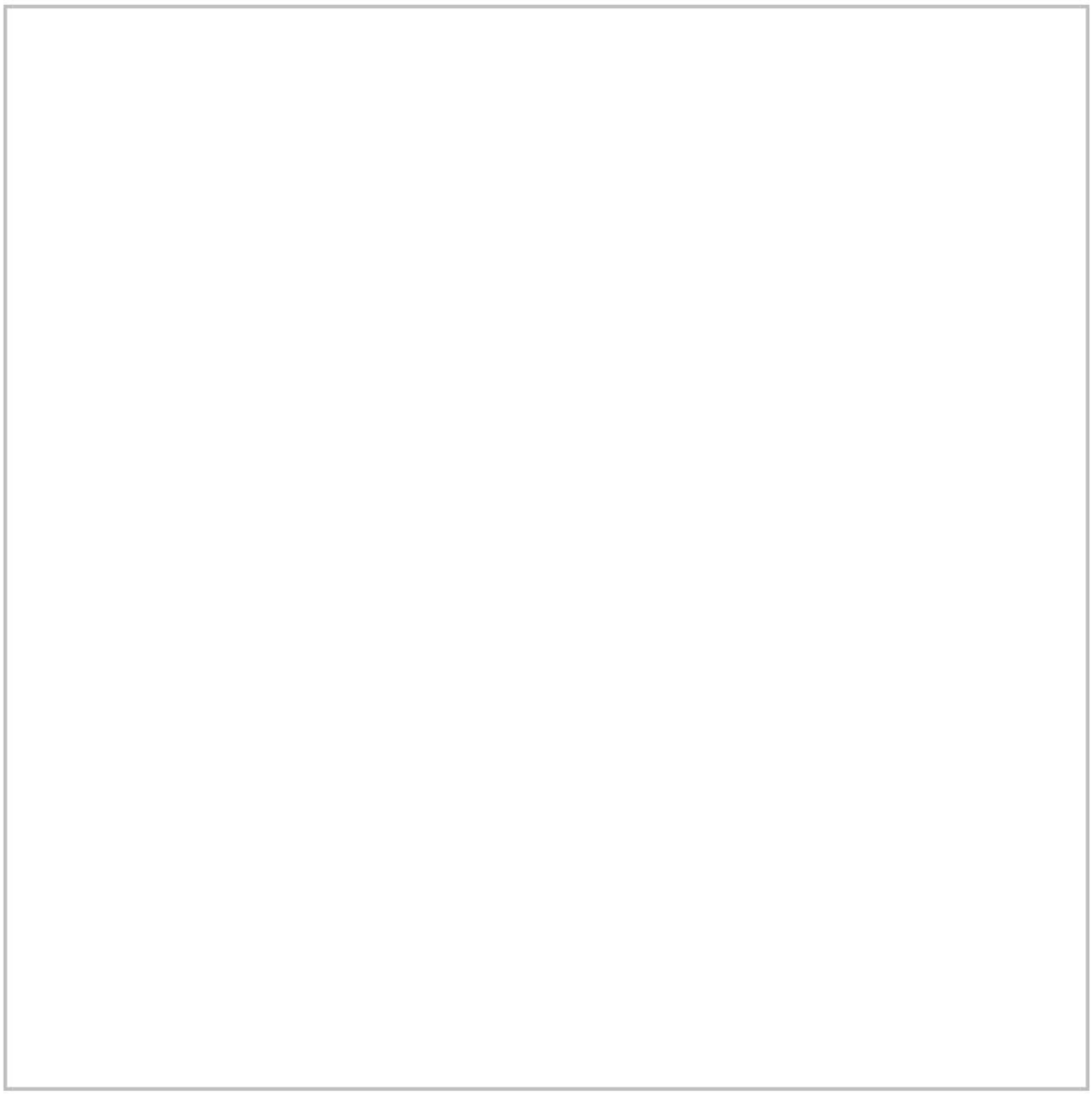
The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE



Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.



Let's Talk Holsters

When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.



2023 Uniform Trends

What law enforcement agencies are buying and what new products to watch.

Integrating Technology: Juggling Public Safety Mission with High-Tech

Going Digital: Harnessing Digital Forensics Technology

The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.

As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION

Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us

This email is being sent to leigha.genduso@pol.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: zzDebuccia, David (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:06:57 PM

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

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

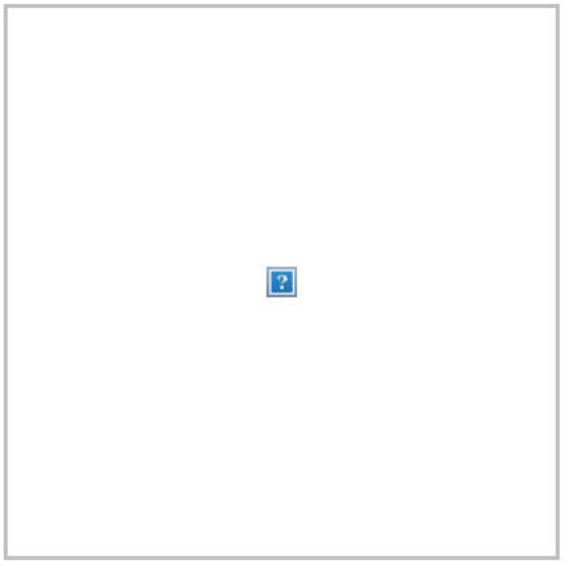
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

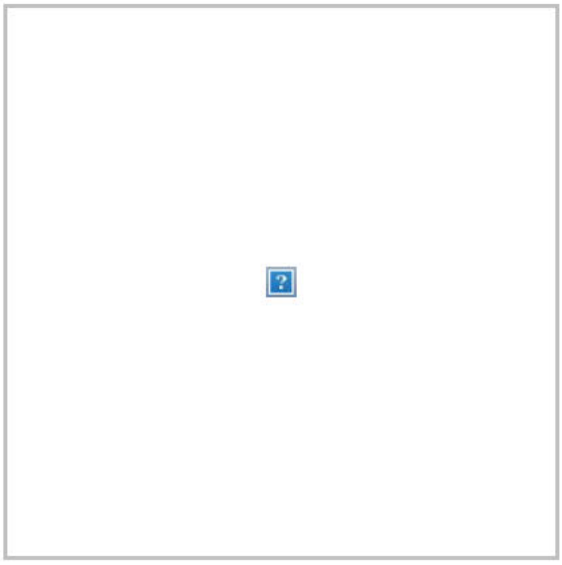
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



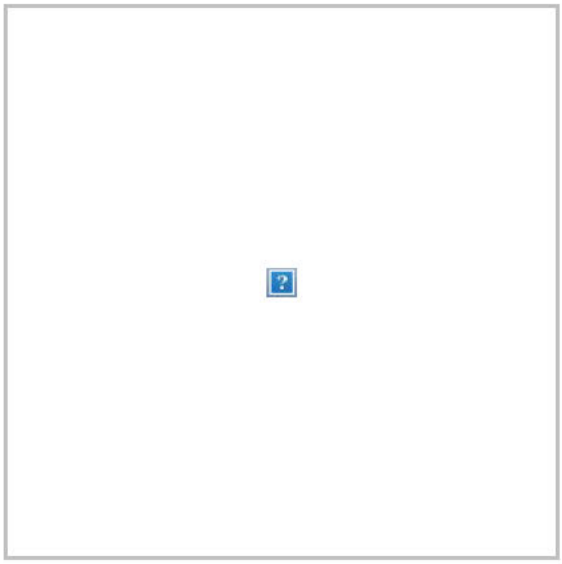
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



V-VICTA

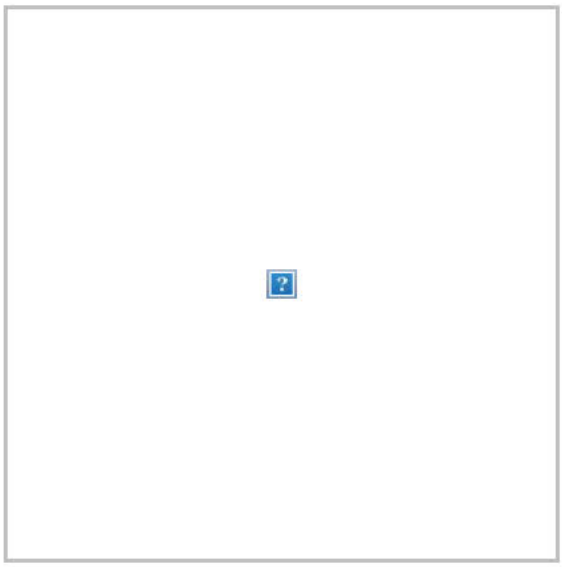
One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

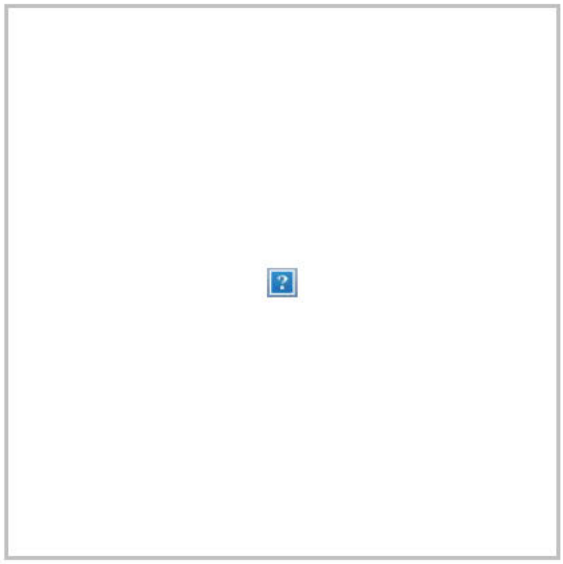
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...

NEW PRODUCTS



Flock Safety Raven

The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem

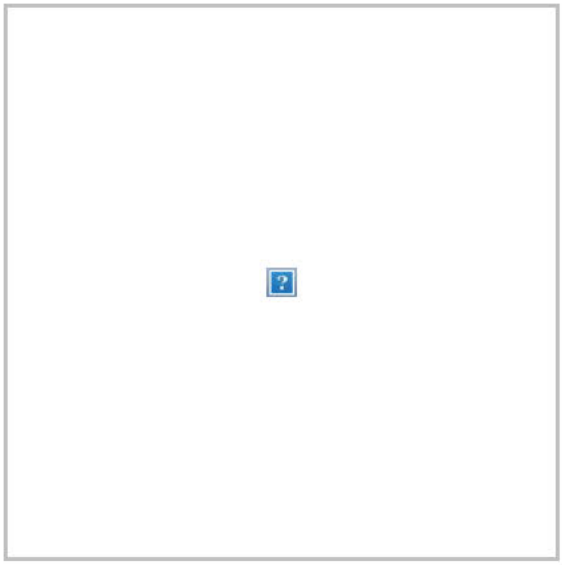


Setina Rear Cargo Storage Box

Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

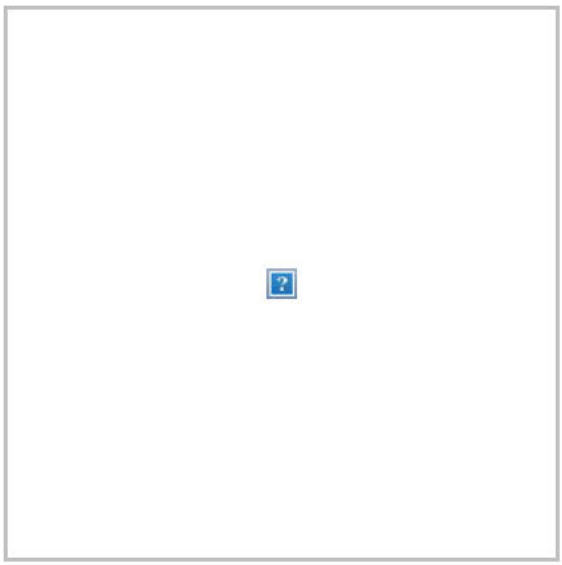


with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

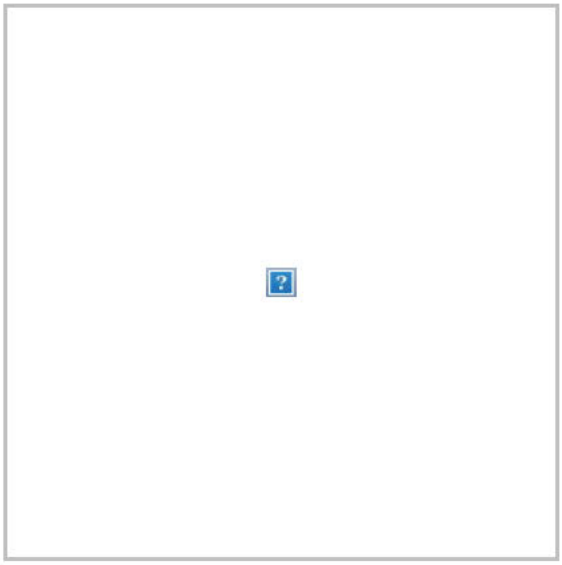


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



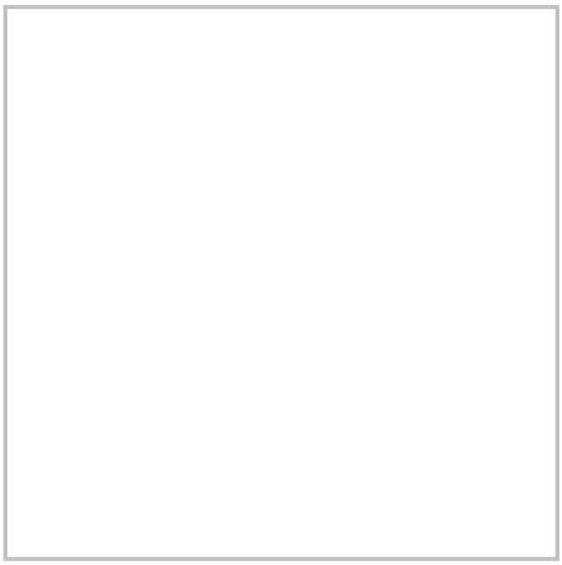
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

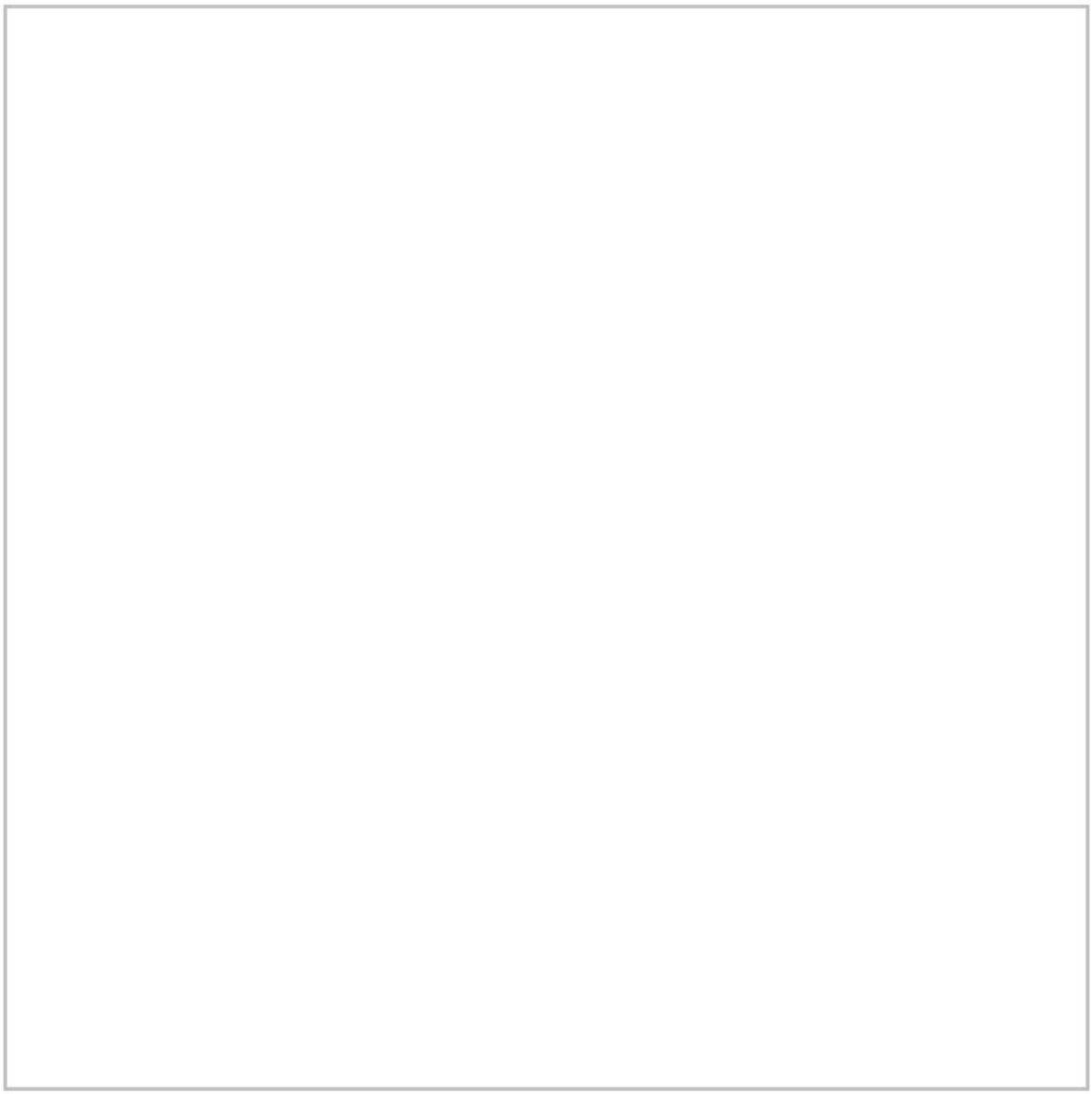
The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE



Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.



Let's Talk Holsters

When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

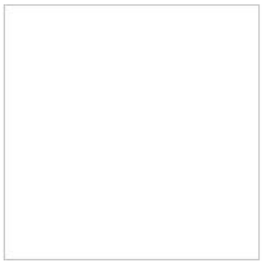
Integrating Technology: Juggling Public Safety Mission with High-Tech



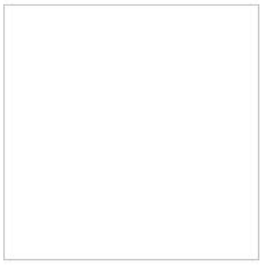
2023 Uniform Trends

What law enforcement agencies are buying and what new products to watch.

Going Digital: Harnessing Digital Forensics Technology

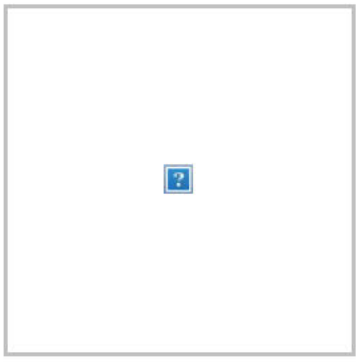


The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.



As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION



Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us



This email is being sent to david.debuccia@pol.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: zzHunter, Richard (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:06:17 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.

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

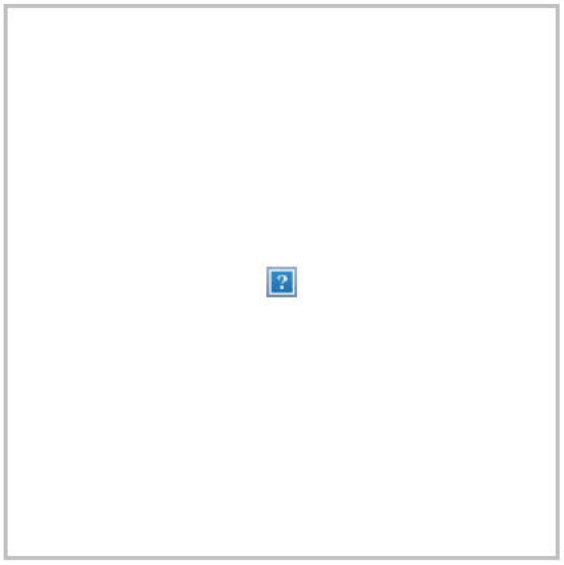
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

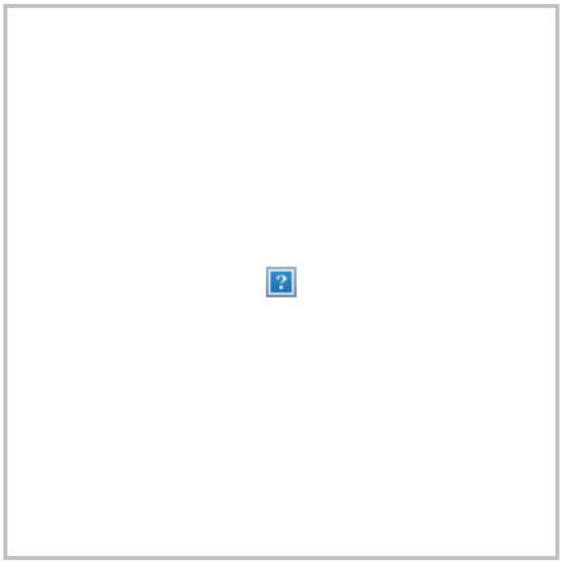
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



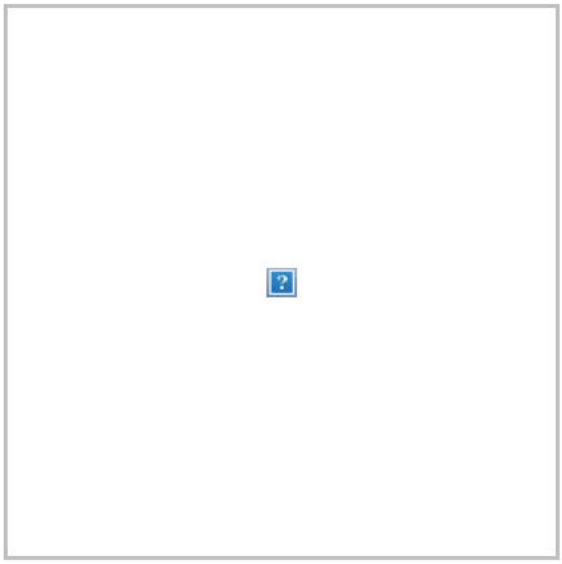
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



V-VICTA

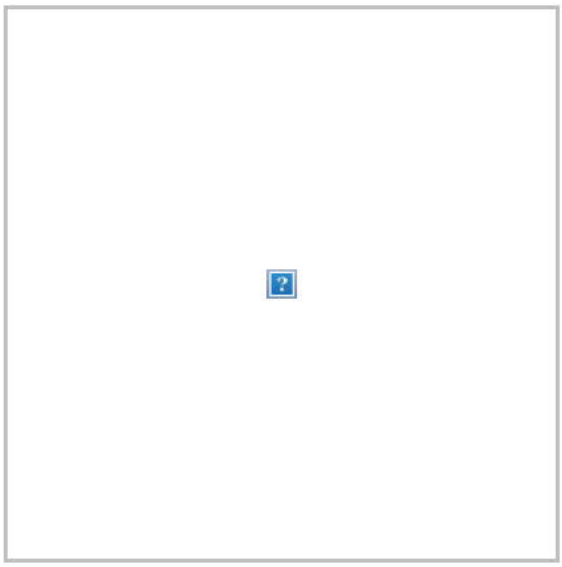
One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

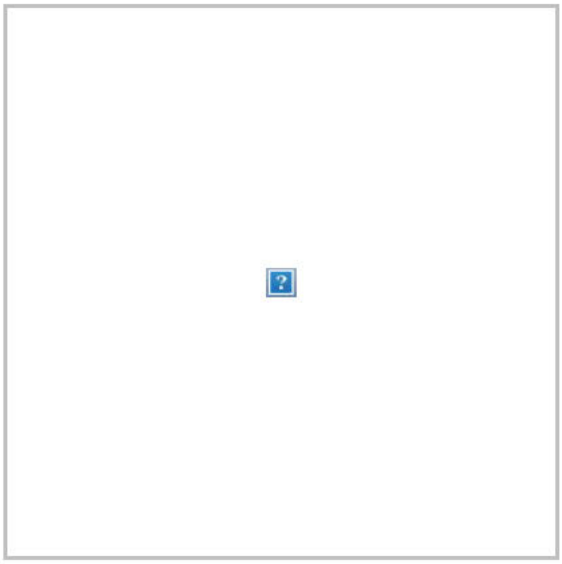
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...

NEW PRODUCTS



Flock Safety Raven

The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem

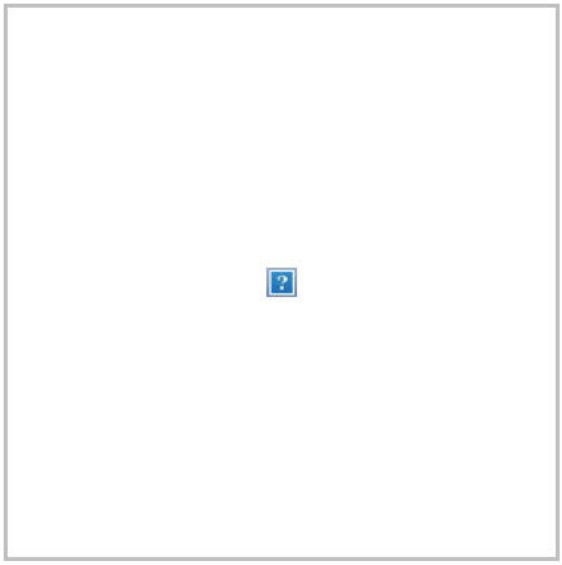


Setina Rear Cargo Storage Box

Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

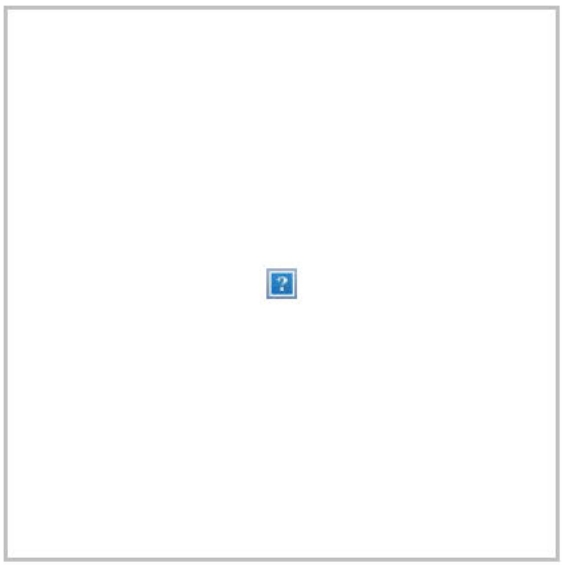


with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

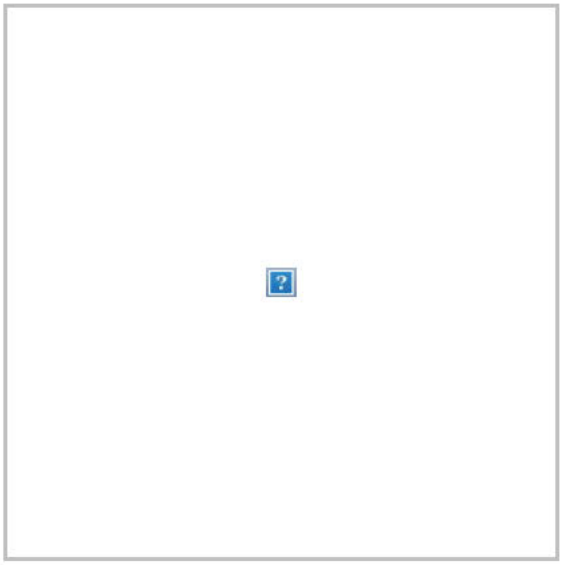


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



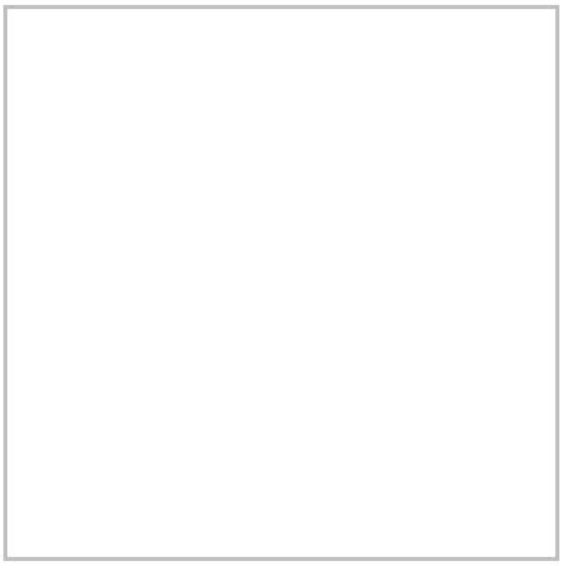
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

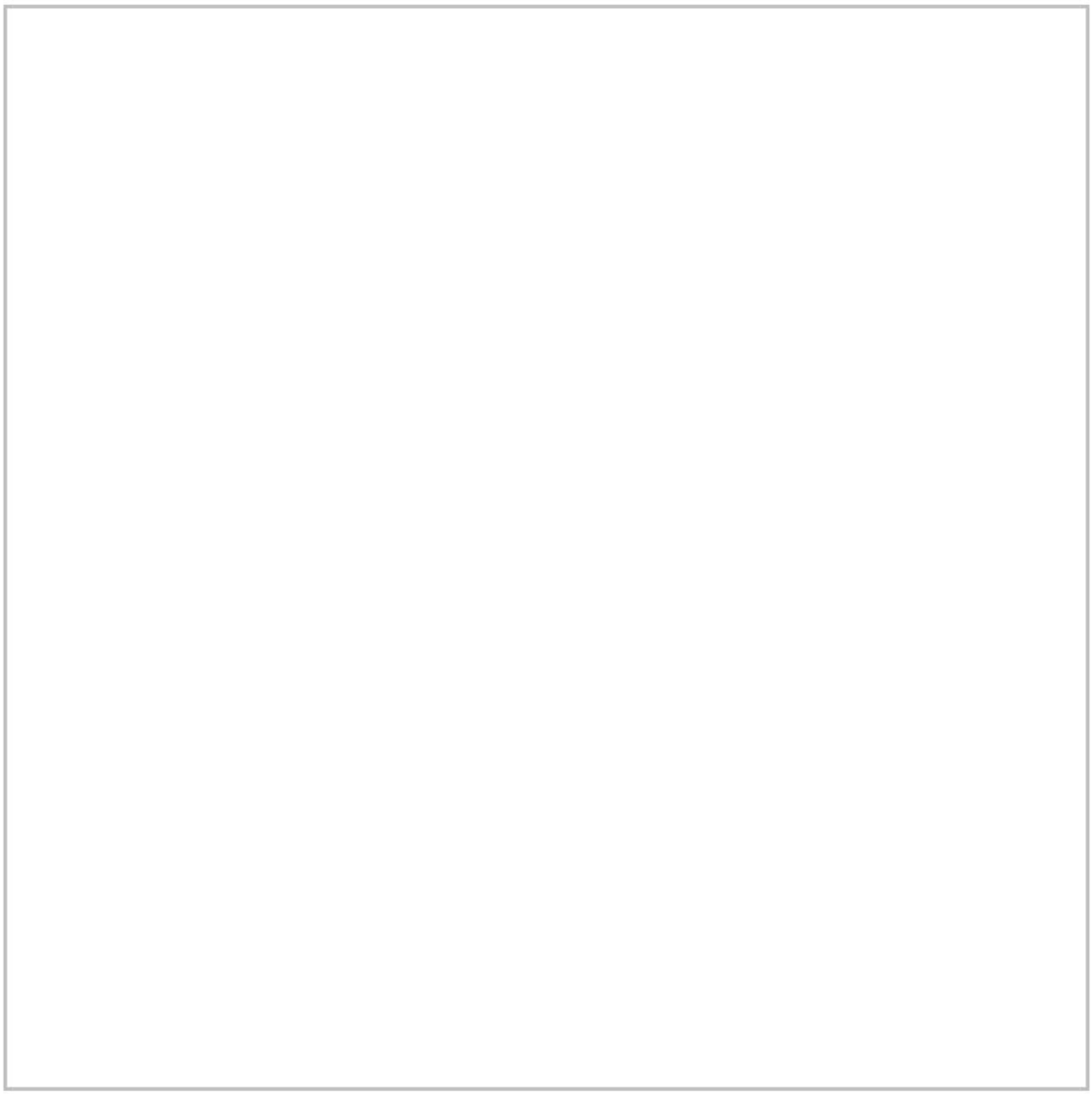
The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE



Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.



Let's Talk Holsters

When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

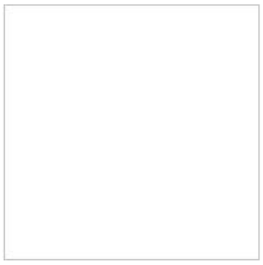
Integrating Technology: Juggling Public Safety Mission with High-Tech



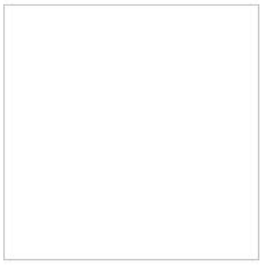
2023 Uniform Trends

What law enforcement agencies are buying and what new products to watch.

Going Digital: Harnessing Digital Forensics Technology

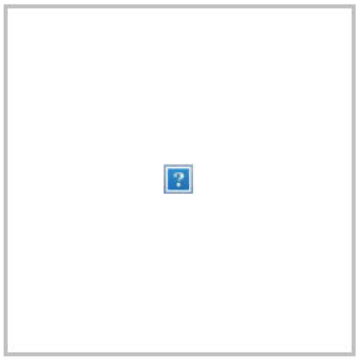


The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.



As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION



Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us



This email is being sent to richard.hunter@pol.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: zzOutwater, Robert (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:06:16 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.

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

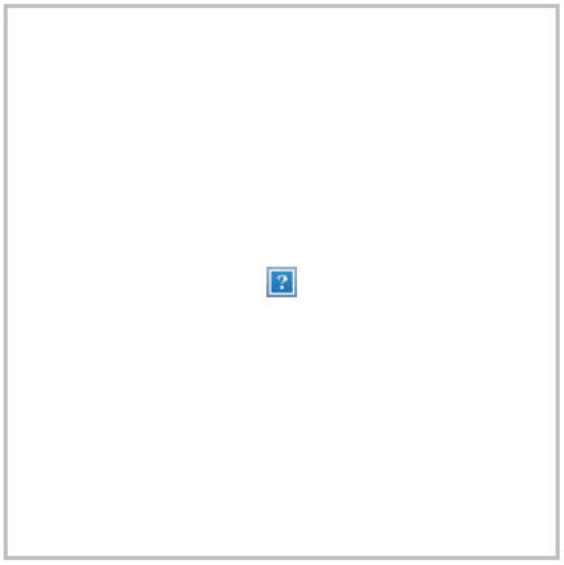
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

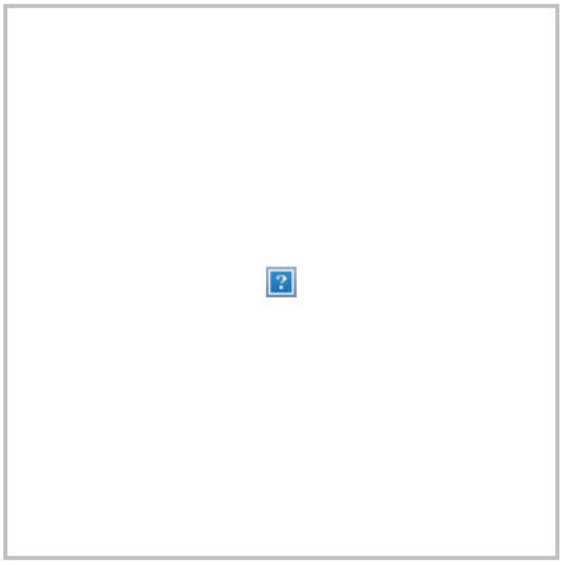
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



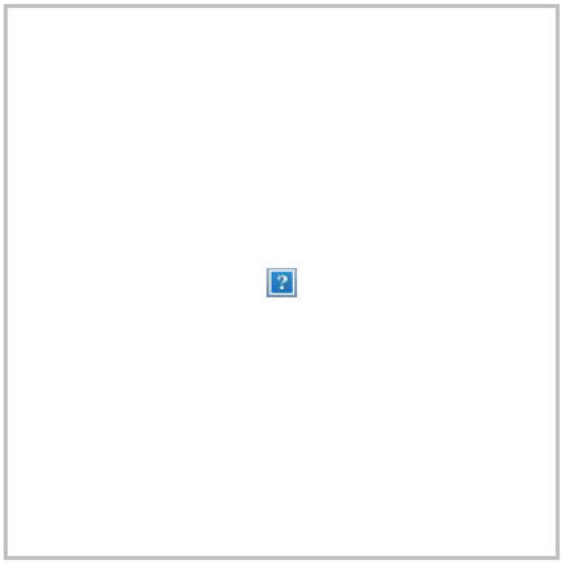
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



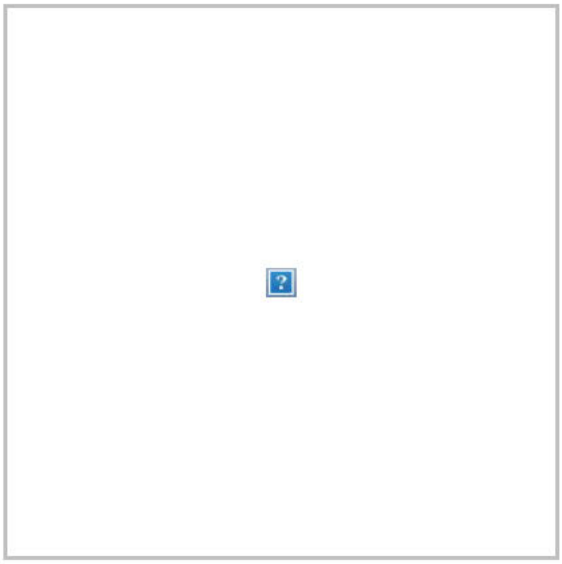
V-VICTA

One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

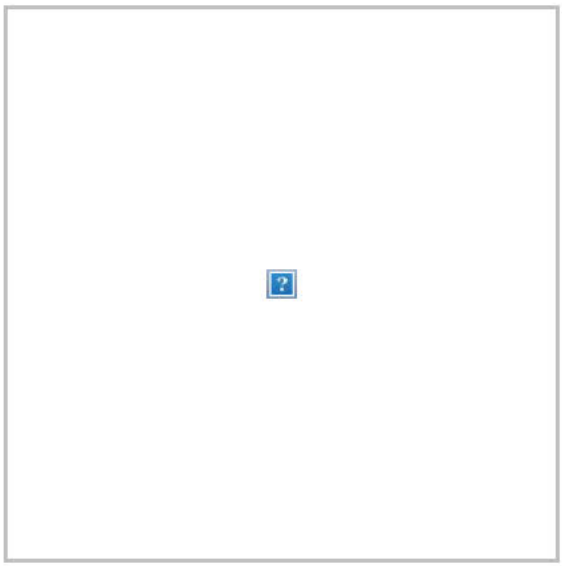
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...



Setina Rear Cargo Storage Box

Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

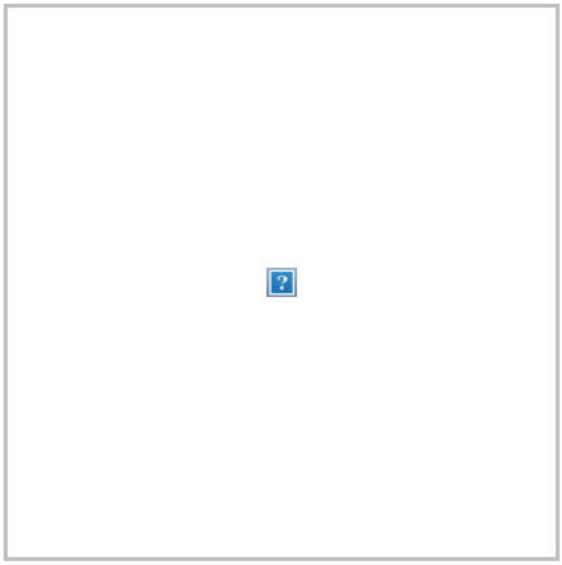
NEW PRODUCTS



Flock Safety Raven

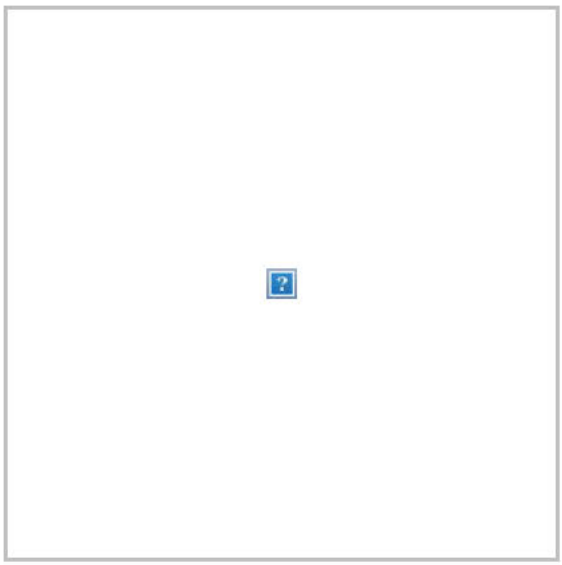
The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem

with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

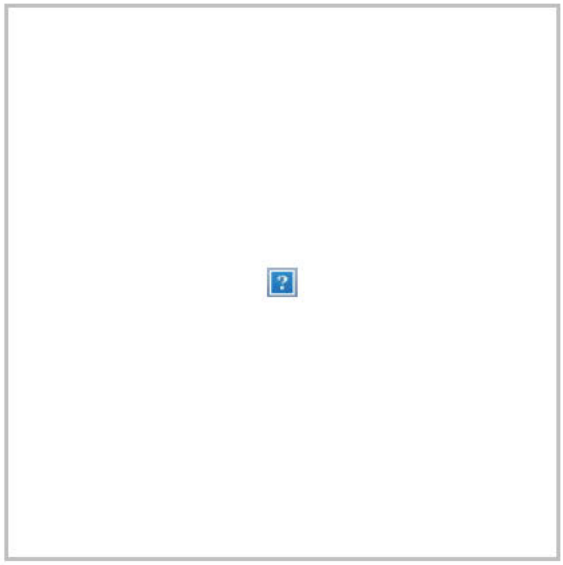


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



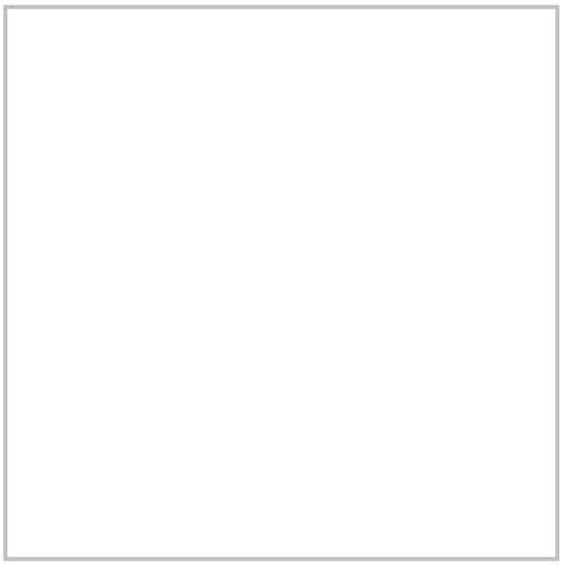
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

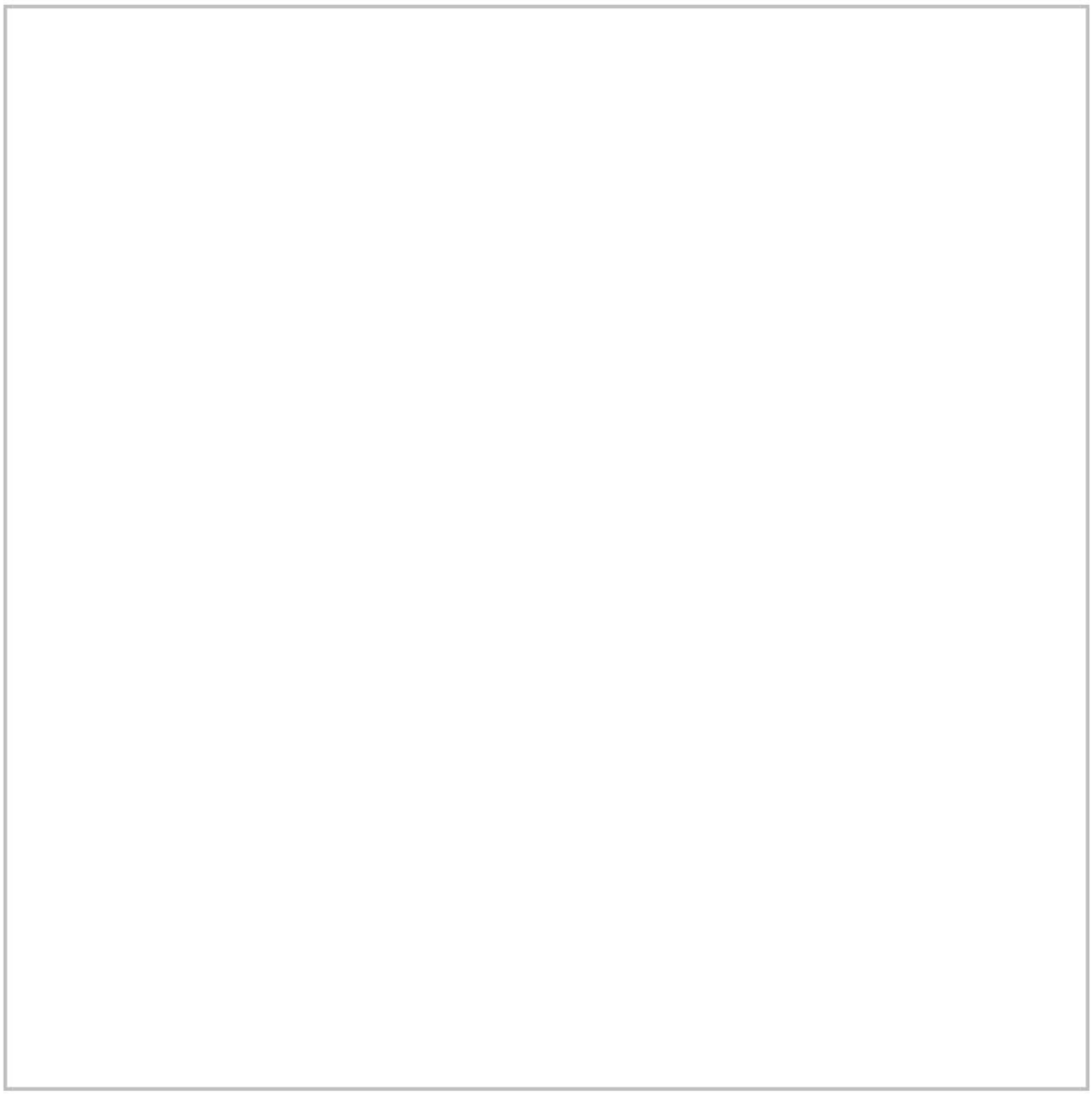
The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE



Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.

Let's Talk Holsters

When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

2023 Uniform Trends

What law enforcement agencies are buying and what new products to watch.

Integrating Technology: Juggling Public Safety Mission with High-Tech

Going Digital: Harnessing Digital Forensics Technology

The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.

As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION

Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us

This email is being sent to robert.outwater@pol.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: Pinkham, John (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:06:10 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.

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

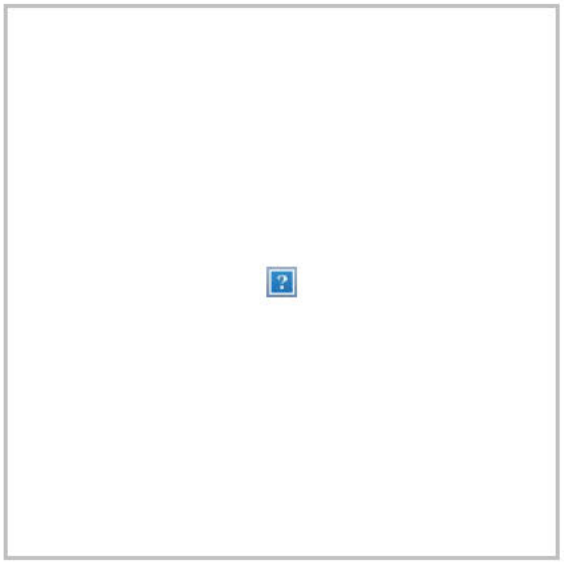
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

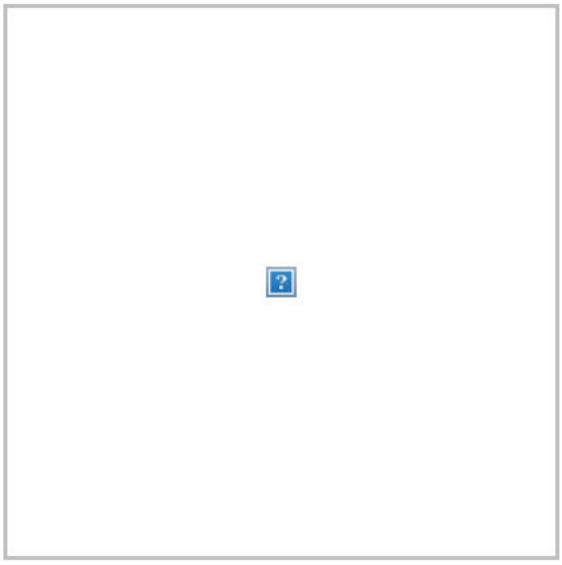
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



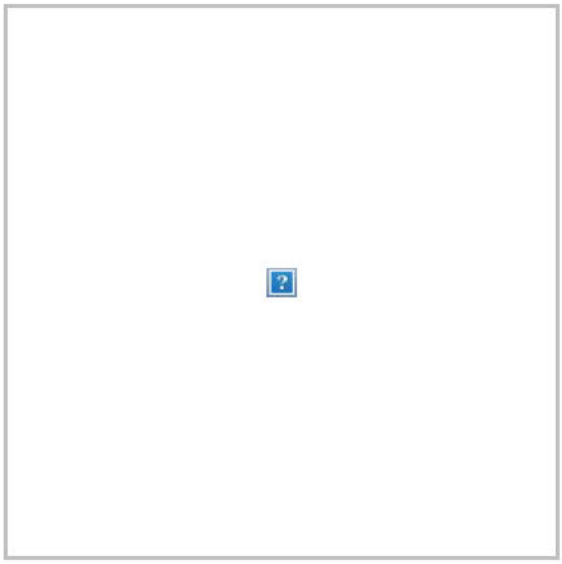
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



V-VICTA

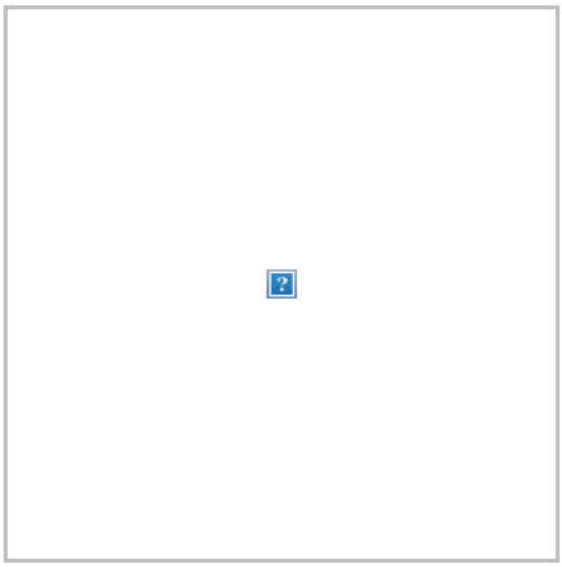
One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

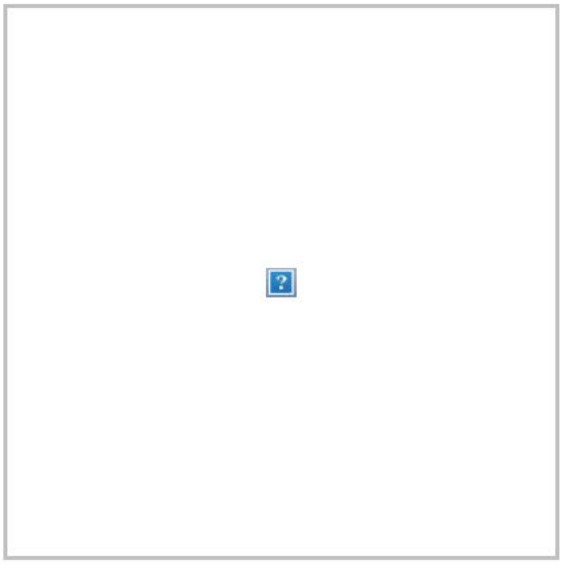
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...

NEW PRODUCTS



Flock Safety Raven

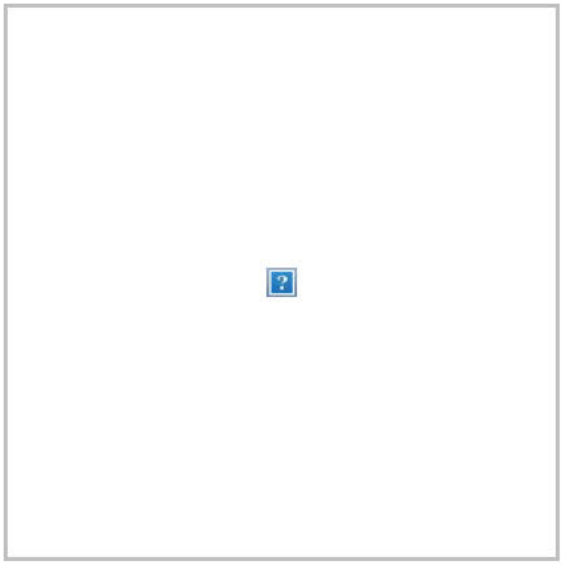
The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem



Setina Rear Cargo Storage Box

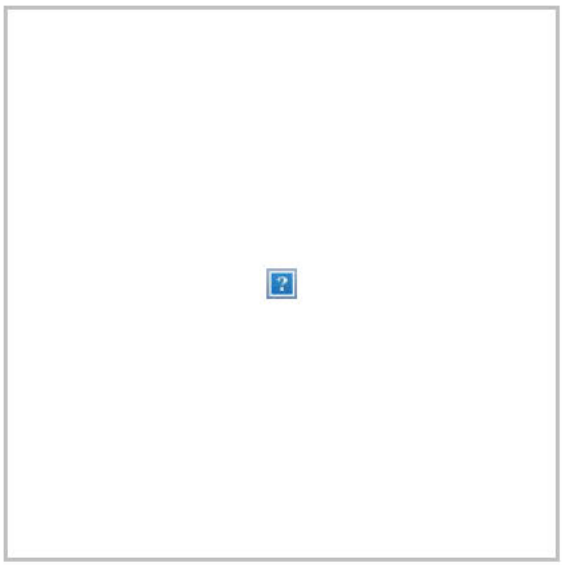
Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

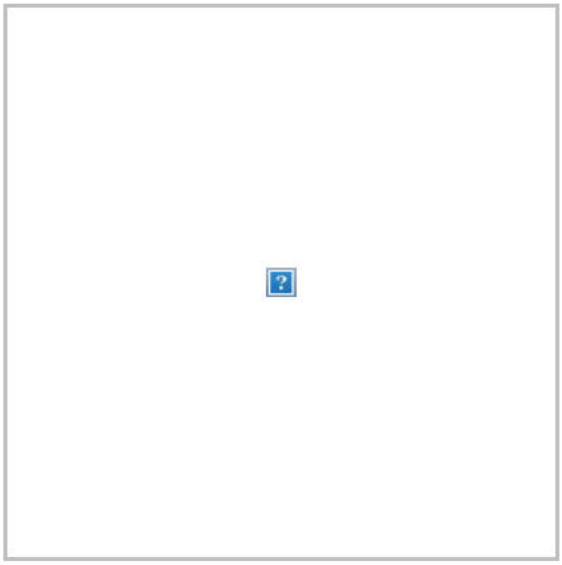


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



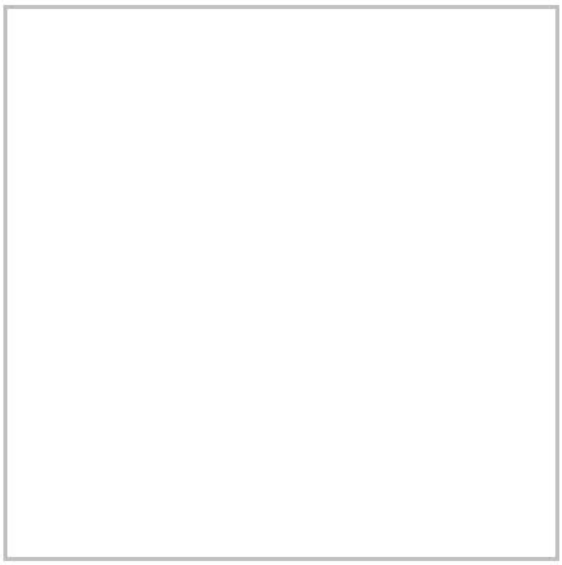
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE

Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.

Let's Talk Holsters

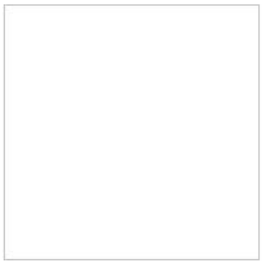
When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

2023 Uniform Trends

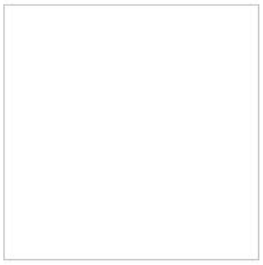
What law enforcement agencies are buying and what new products to watch.

Integrating Technology: Juggling Public Safety Mission with High-Tech

Going Digital: Harnessing Digital Forensics Technology

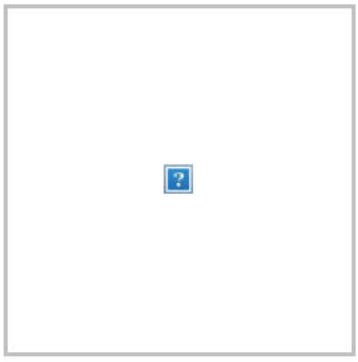


The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.



As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION



Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us



This email is being sent to john.pinkham@massmail.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: Carriere, Anthony (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:06:02 PM

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

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

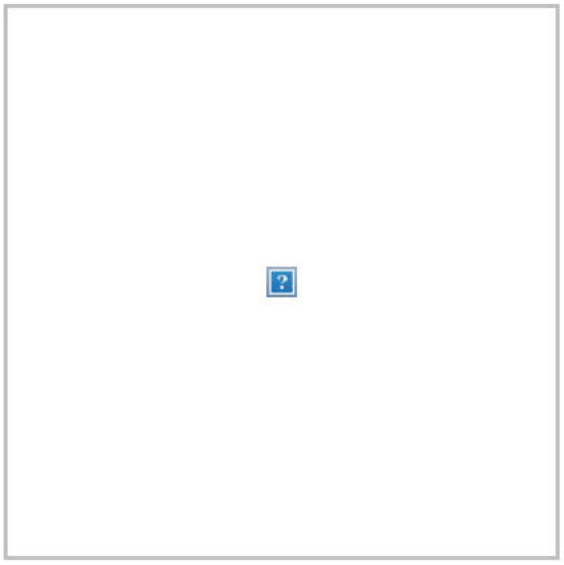
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

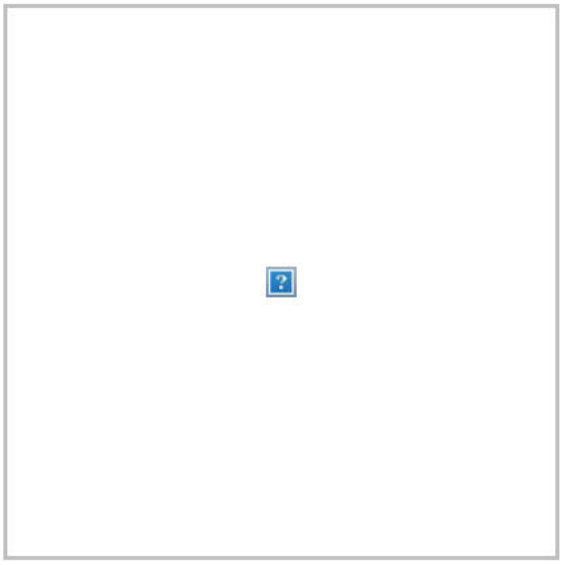
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



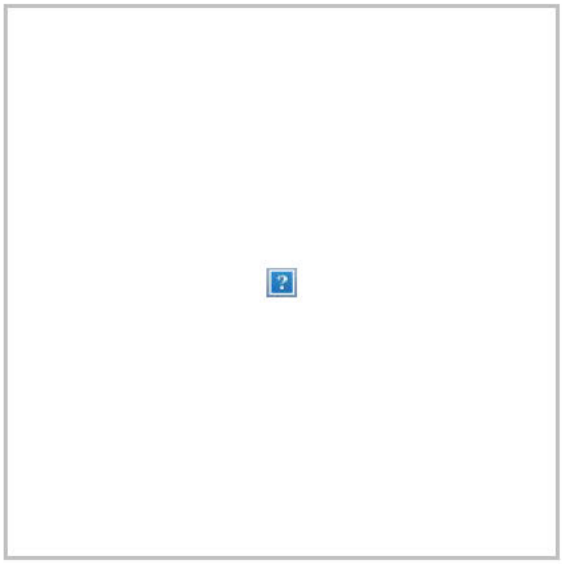
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



V-VICTA

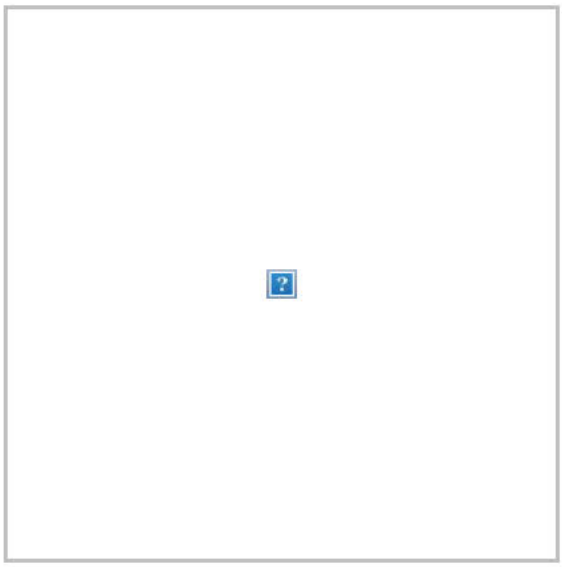
One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

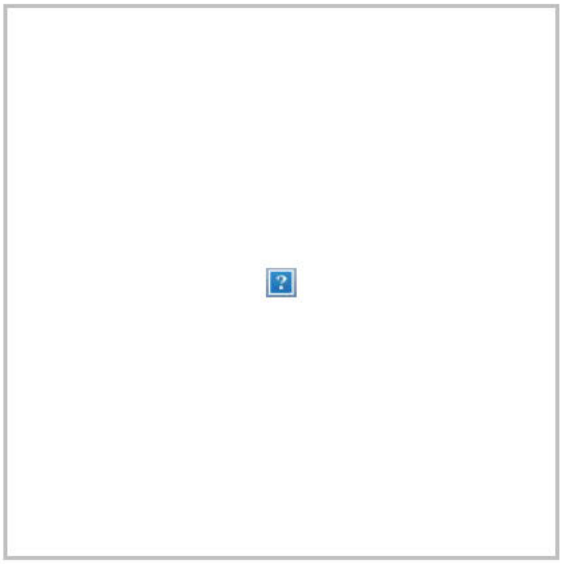
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...

NEW PRODUCTS



Flock Safety Raven

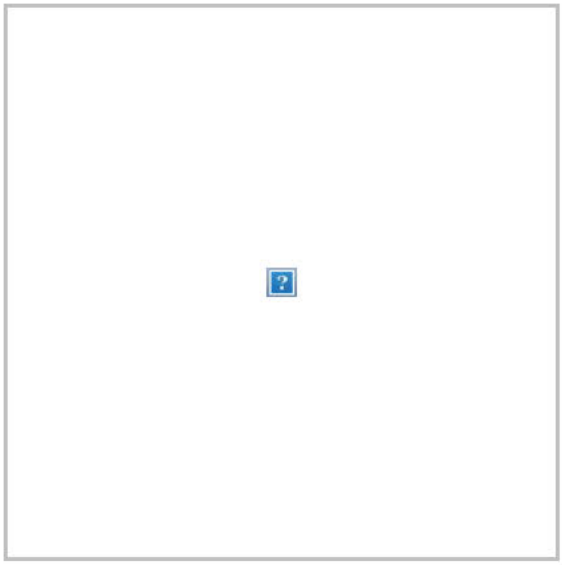
The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem



Setina Rear Cargo Storage Box

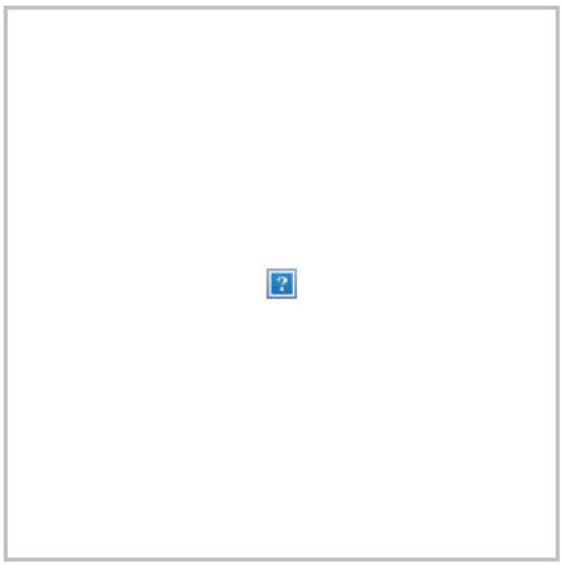
Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

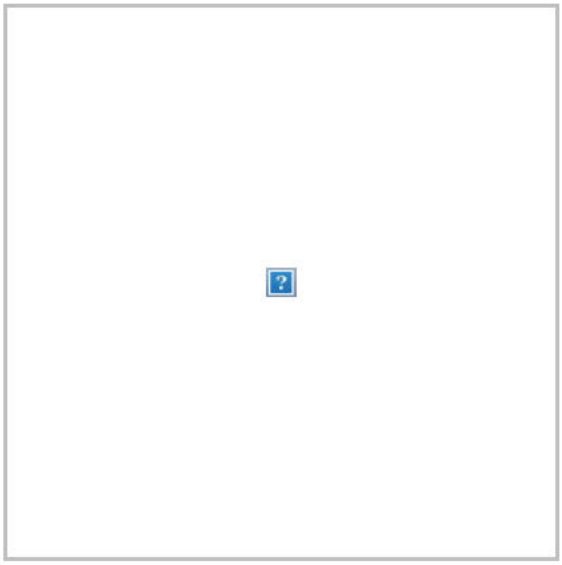


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



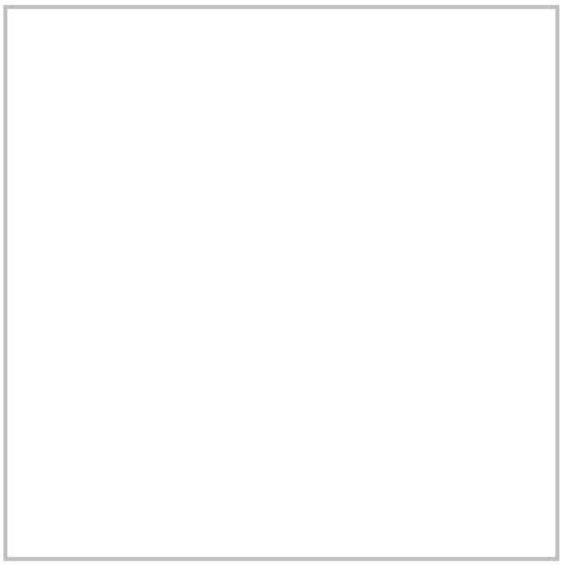
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE

Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.

Let's Talk Holsters

When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

2023 Uniform Trends

What law enforcement agencies are buying and what new products to watch.

Integrating Technology: Juggling Public Safety Mission with High-Tech

Going Digital: Harnessing Digital Forensics Technology

The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.

As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION

Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us

This email is being sent to anthony.carriere@pol.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: Curtin, Timothy (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:05:57 PM

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

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

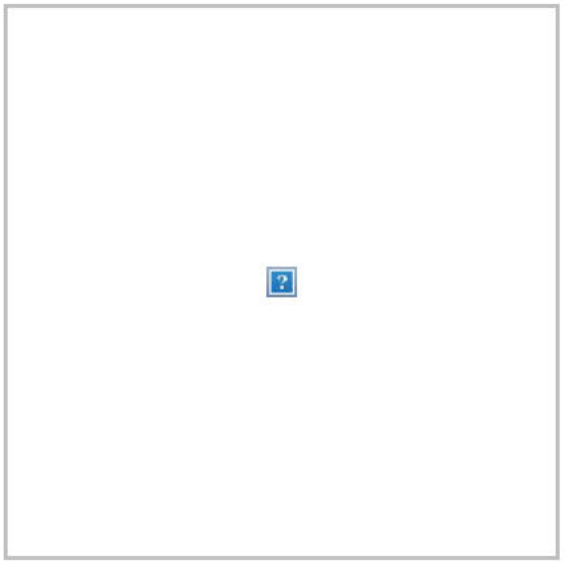
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

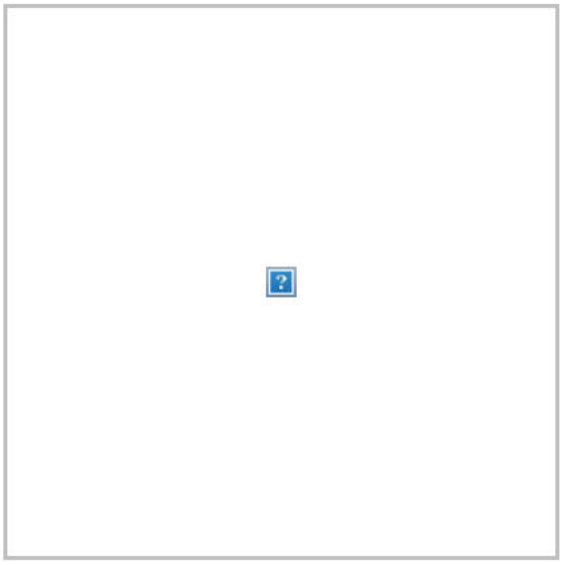
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



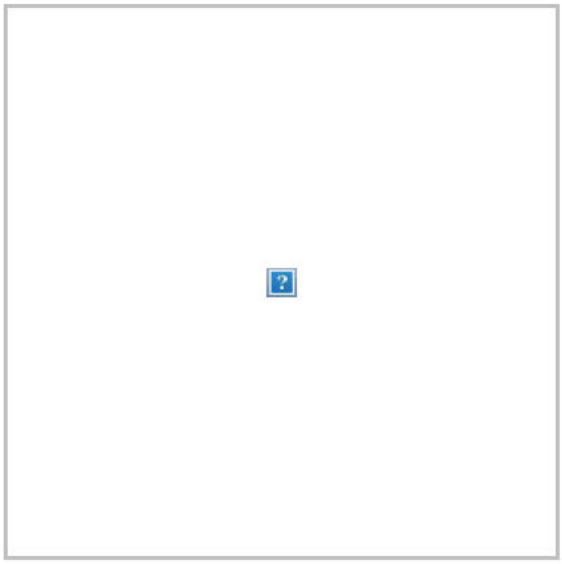
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



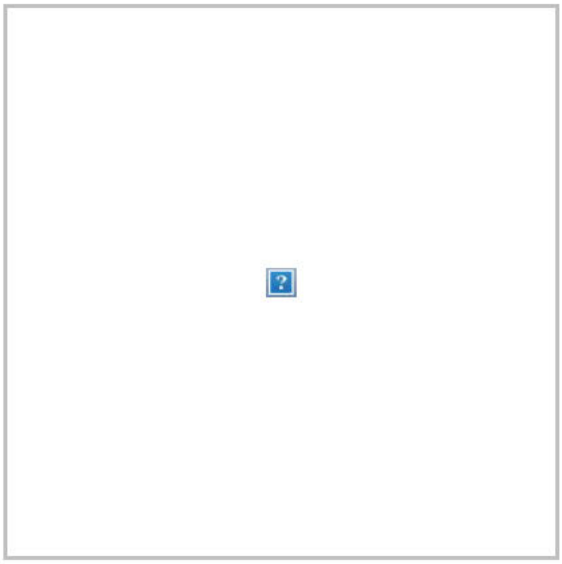
V-VICTA

One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

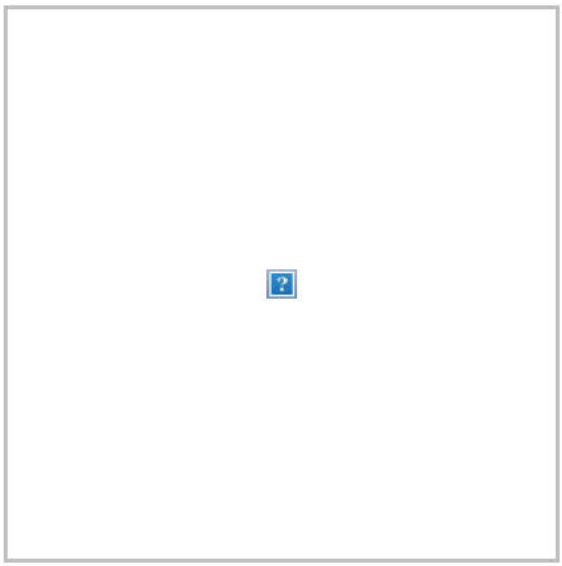
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...



Setina Rear Cargo Storage Box

Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

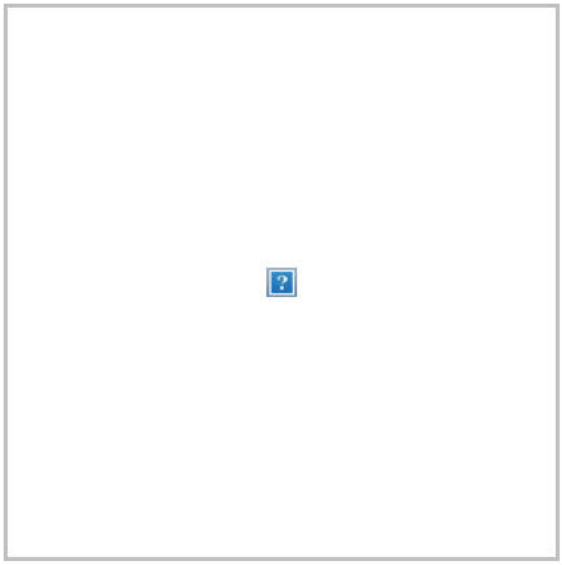
NEW PRODUCTS



Flock Safety Raven

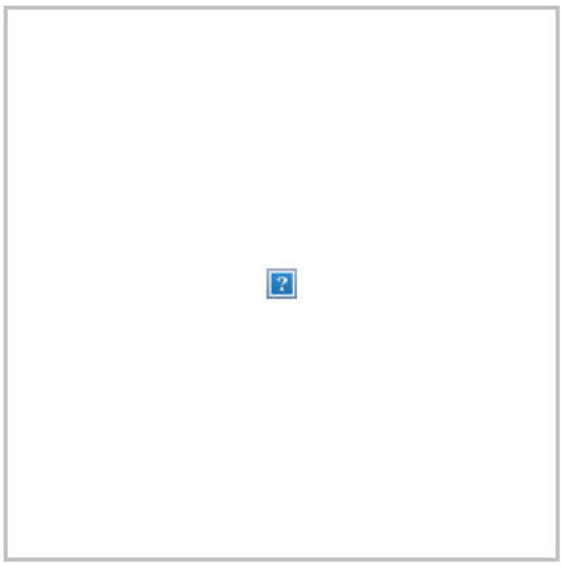
The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem

with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

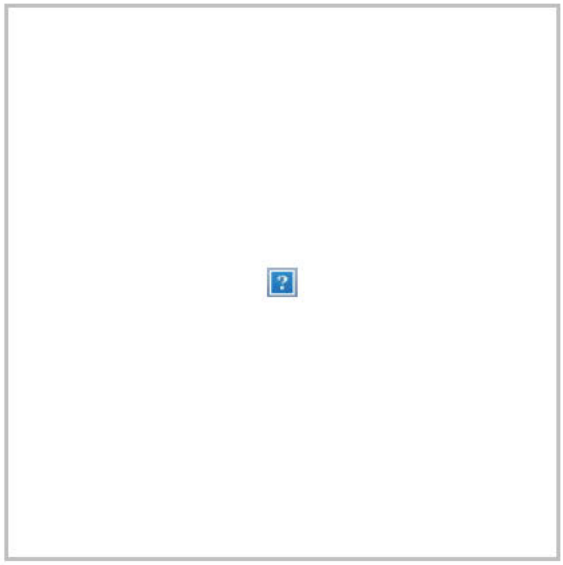


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



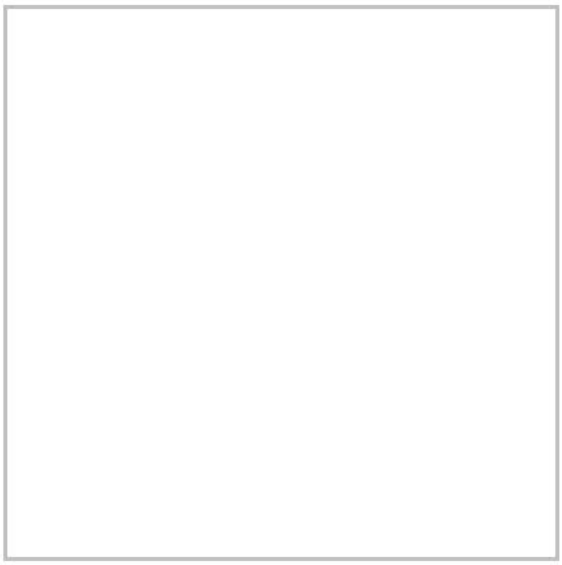
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE

Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.

Let's Talk Holsters

When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

2023 Uniform Trends

What law enforcement agencies are buying and what new products to watch.

Integrating Technology: Juggling Public Safety Mission with High-Tech

Going Digital: Harnessing Digital Forensics Technology

The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.

As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION

Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us

This email is being sent to timothy.curtin@state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: Procopio, David (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:05:29 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.

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

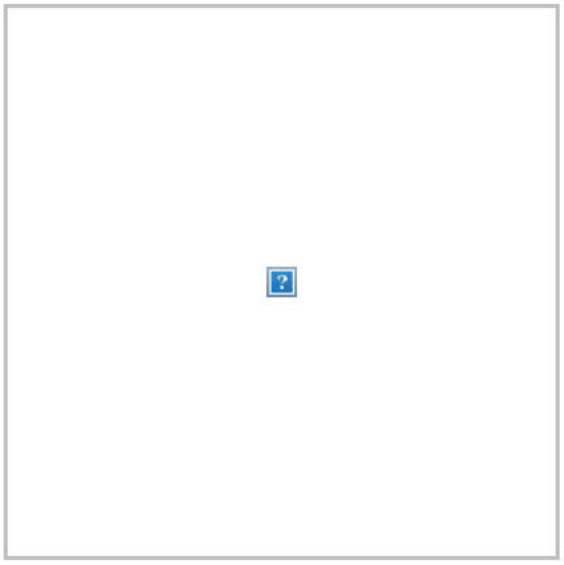
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

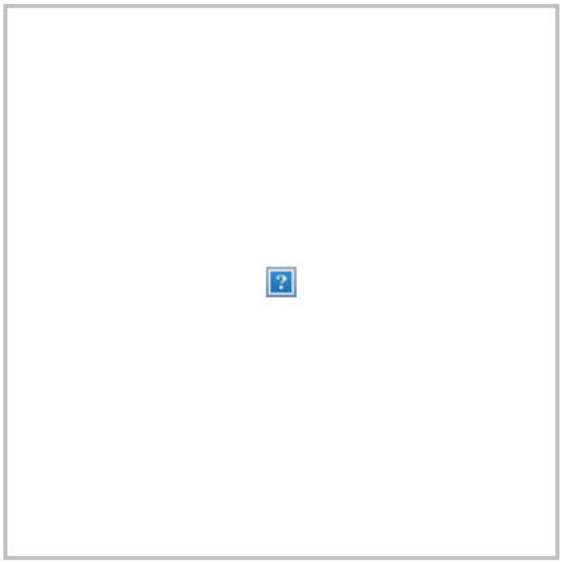
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



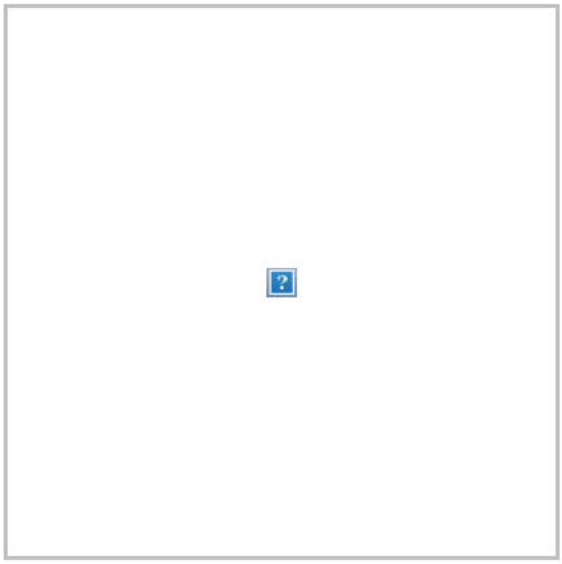
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



V-VICTA

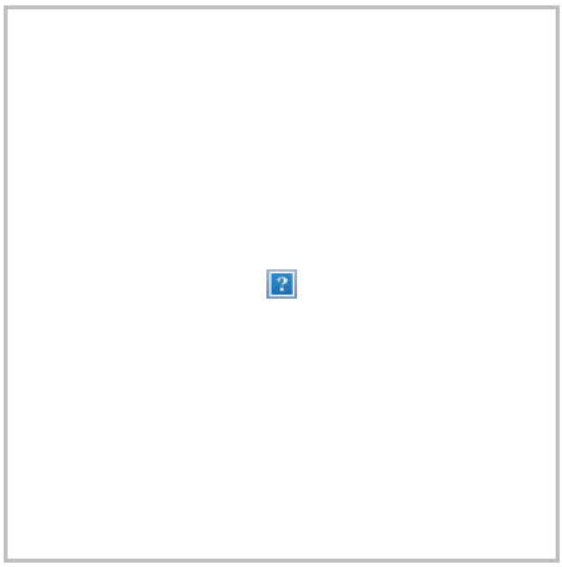
One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

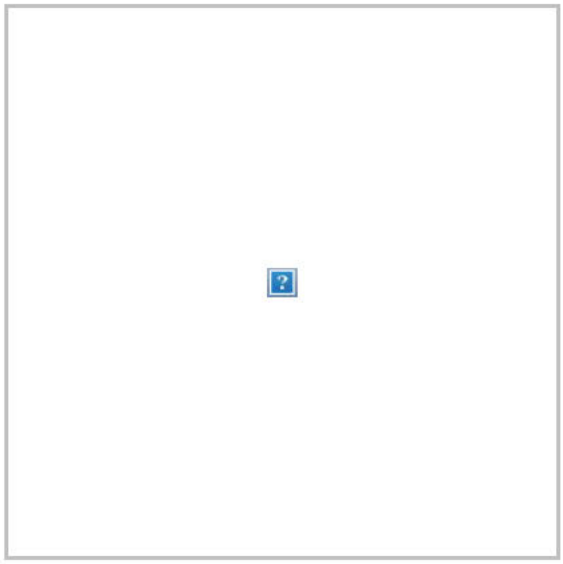
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...

NEW PRODUCTS



Flock Safety Raven

The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem

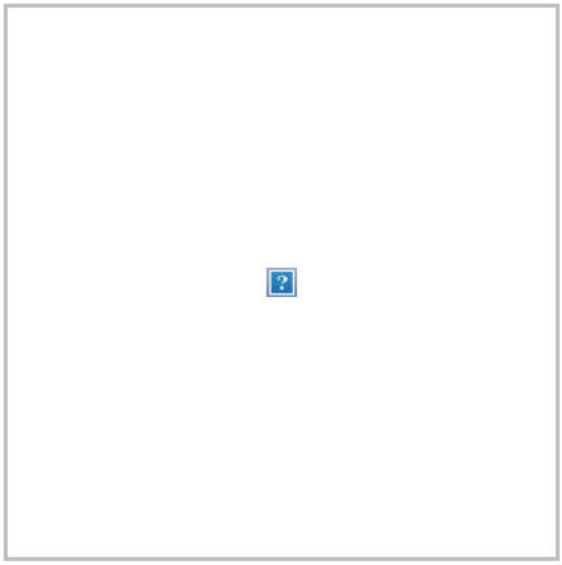


Setina Rear Cargo Storage Box

Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

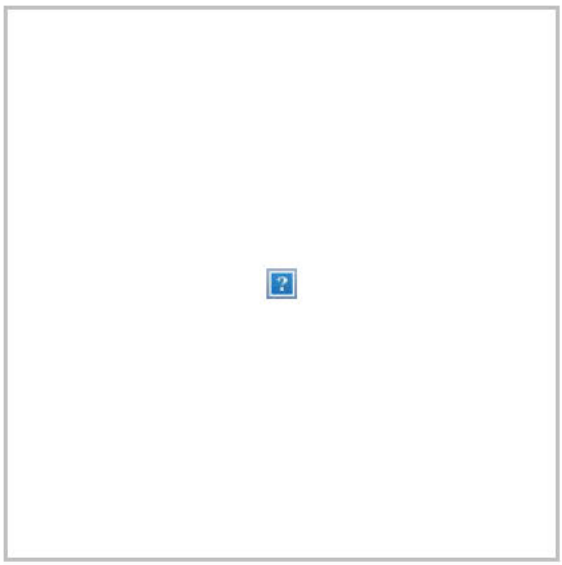


with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

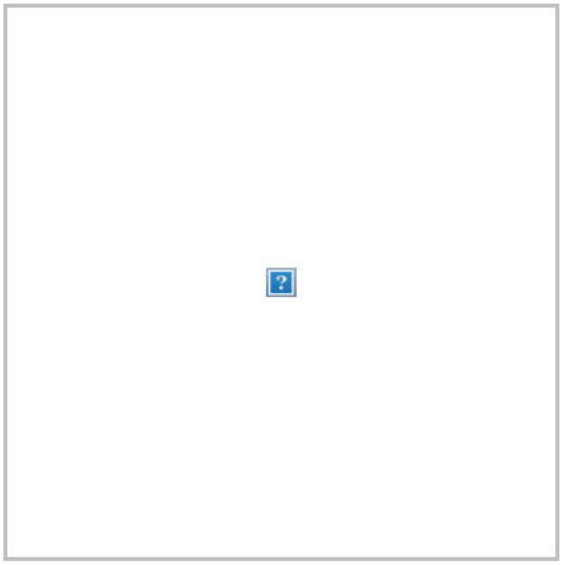


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



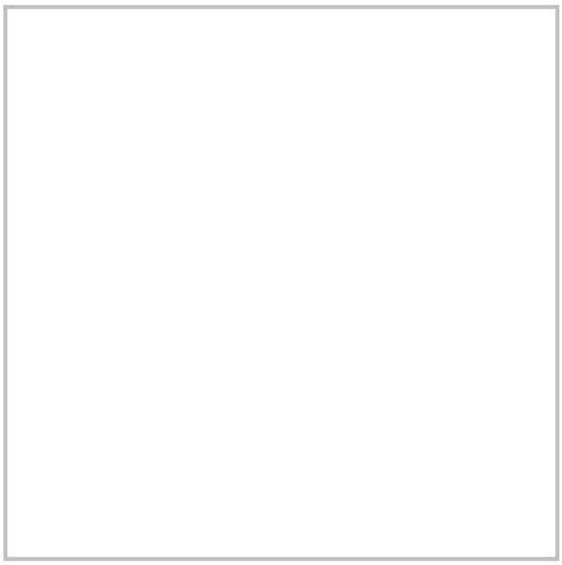
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE

Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.

Let's Talk Holsters

When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

2023 Uniform Trends

What law enforcement agencies are buying and what new products to watch.

Integrating Technology: Juggling Public Safety Mission with High-Tech

Going Digital: Harnessing Digital Forensics Technology

The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.

As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION

Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us

This email is being sent to david.procopio@pol.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: zzMaloney, Sean (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:04:55 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.

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

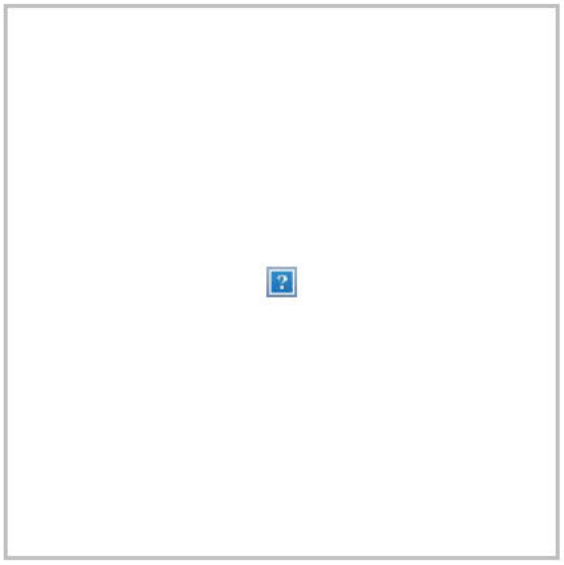
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

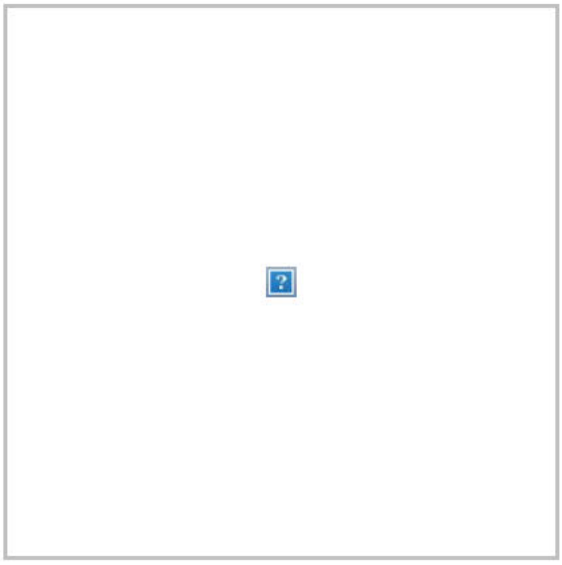
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



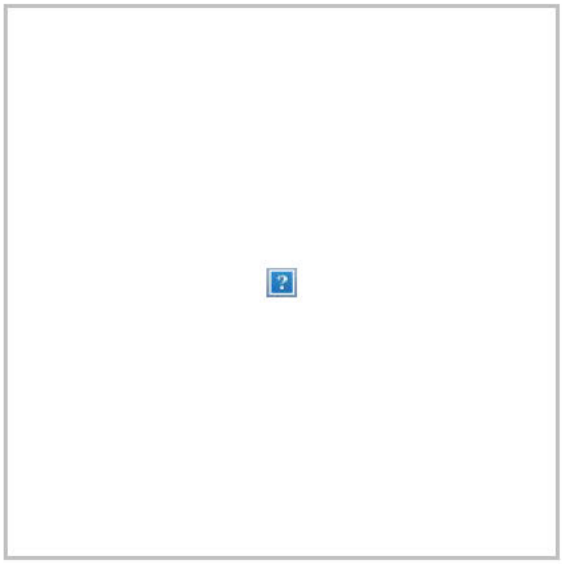
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



V-VICTA

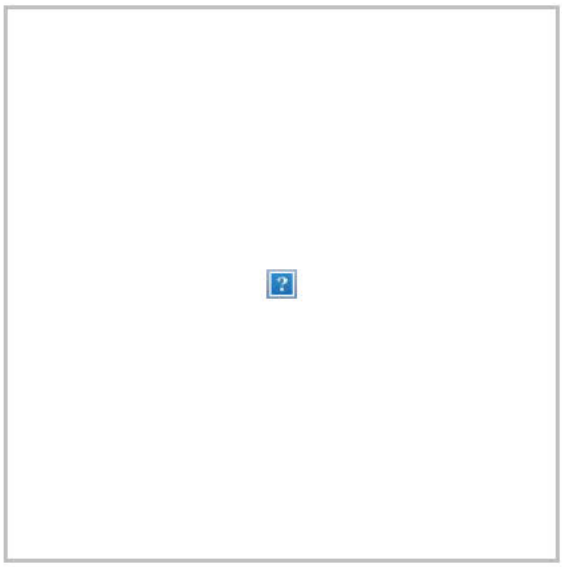
One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

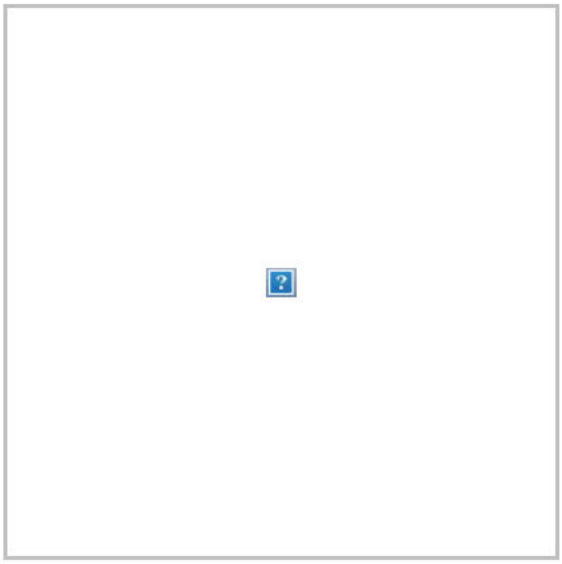
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...

NEW PRODUCTS



Flock Safety Raven

The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem

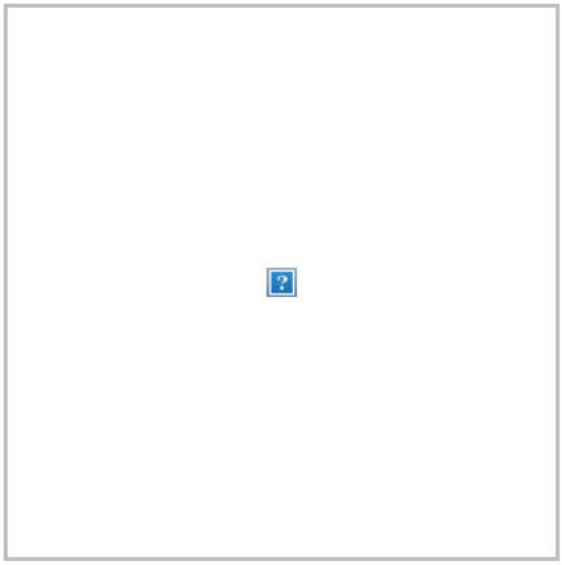


Setina Rear Cargo Storage Box

Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

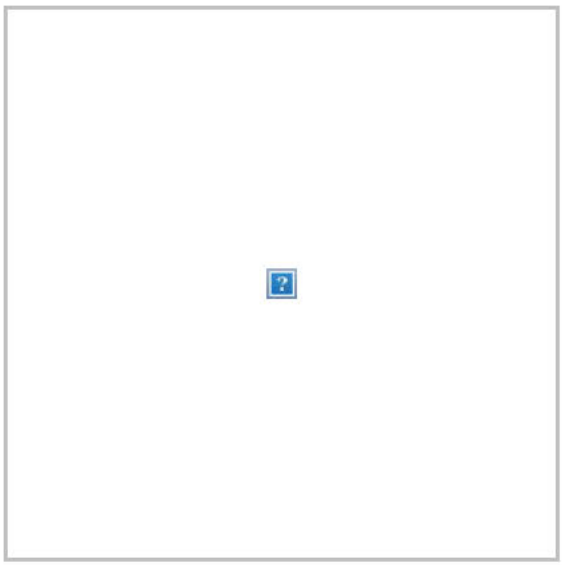


with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

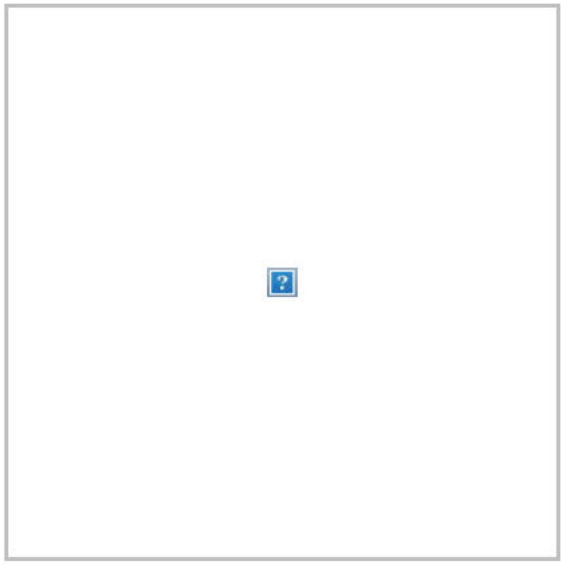


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



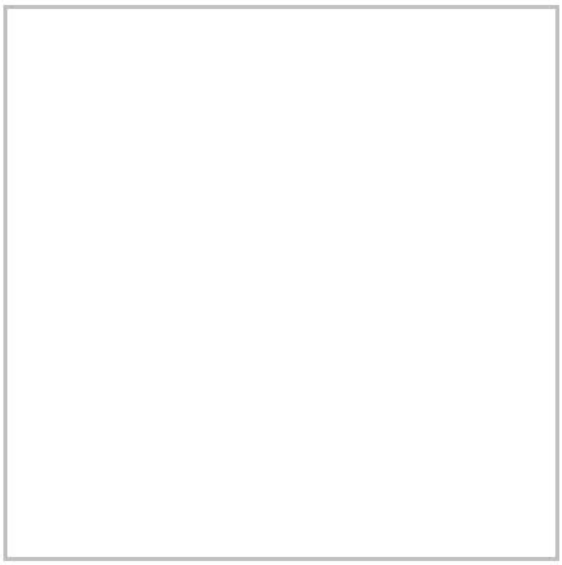
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

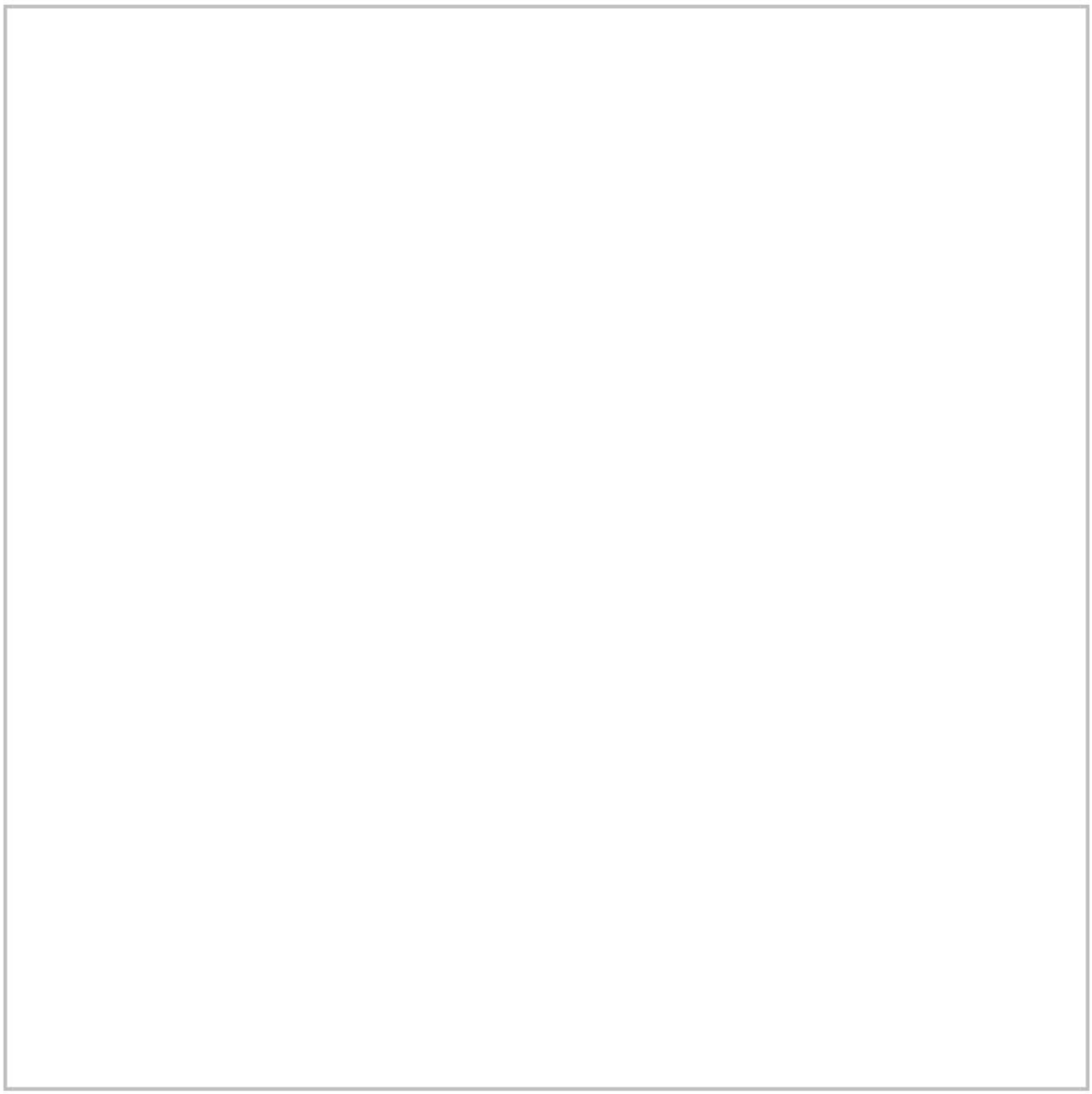
The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE



Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.



Let's Talk Holsters

When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

Integrating Technology: Juggling Public Safety Mission with High-Tech



2023 Uniform Trends

What law enforcement agencies are buying and what new products to watch.

Going Digital: Harnessing Digital Forensics Technology

The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.

As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION

Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us

This email is being sent to sean.maloney@pol.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: Bakey, Thomas (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:03:35 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.

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

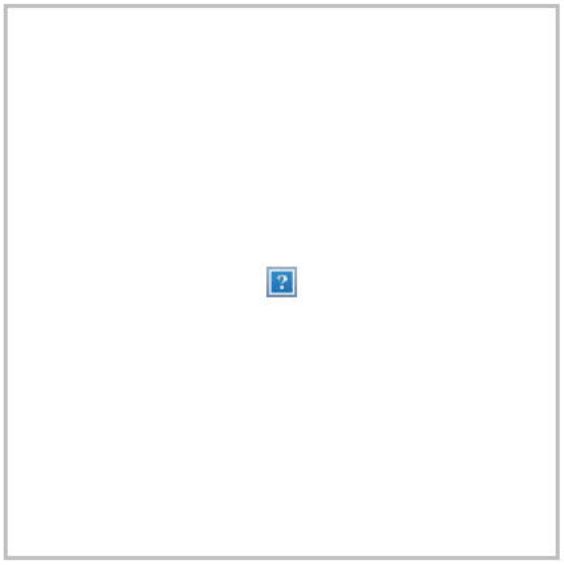
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

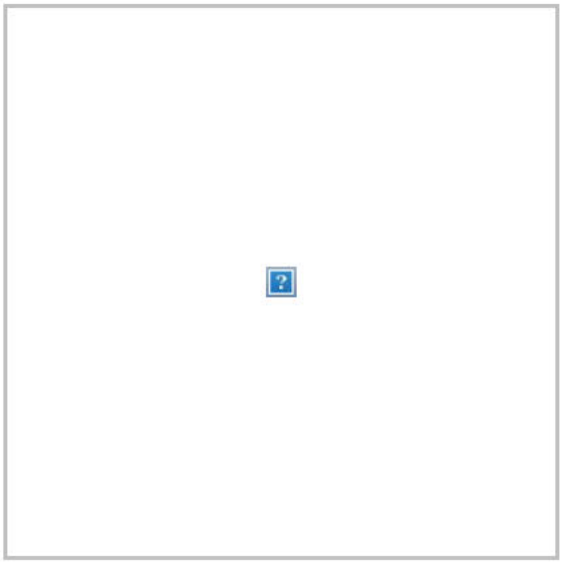
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



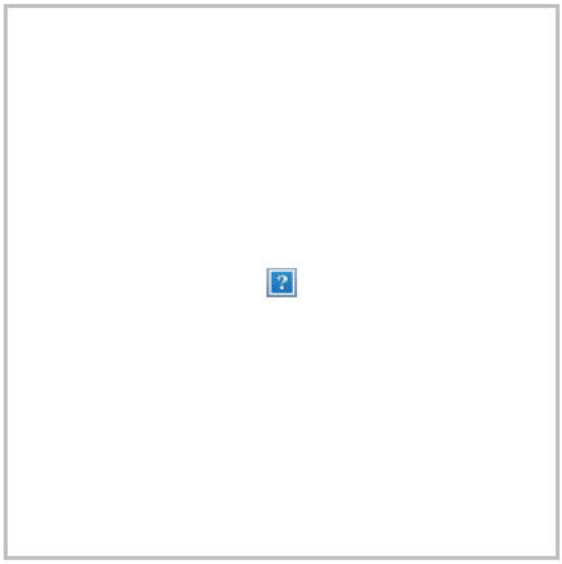
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



V-VICTA

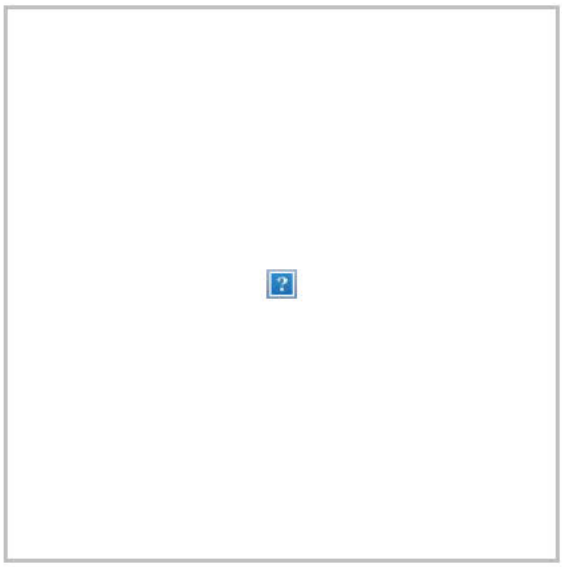
One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

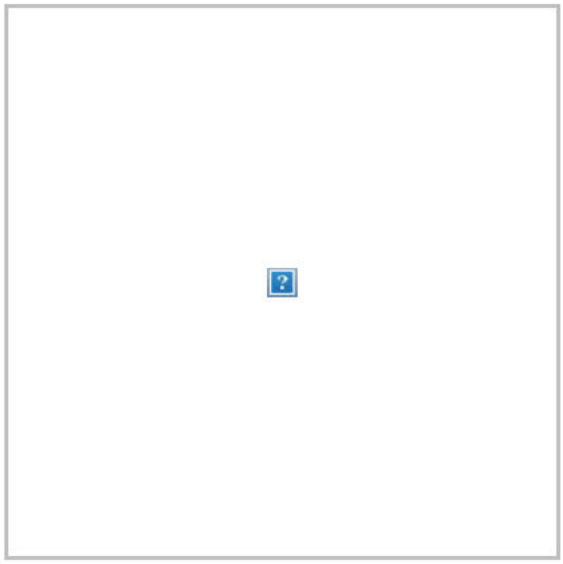
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...

NEW PRODUCTS



Flock Safety Raven

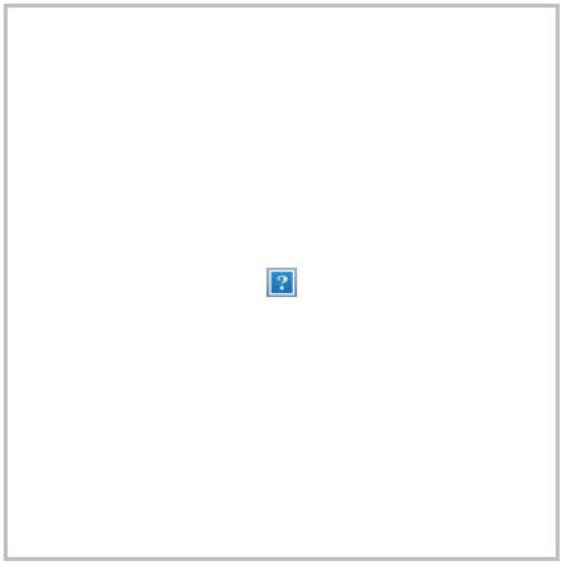
The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem



Setina Rear Cargo Storage Box

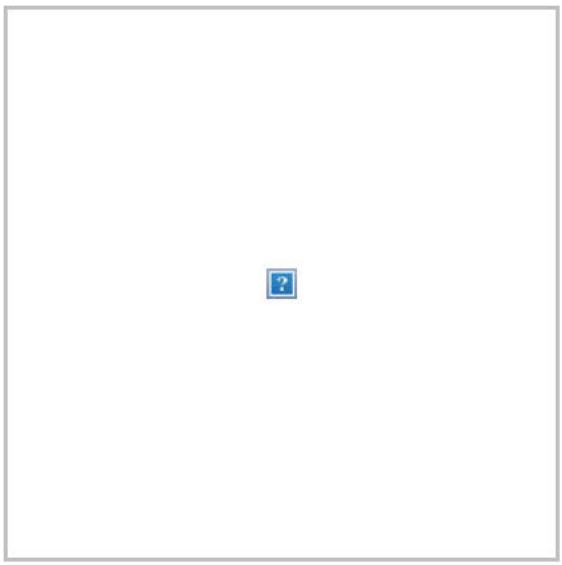
Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

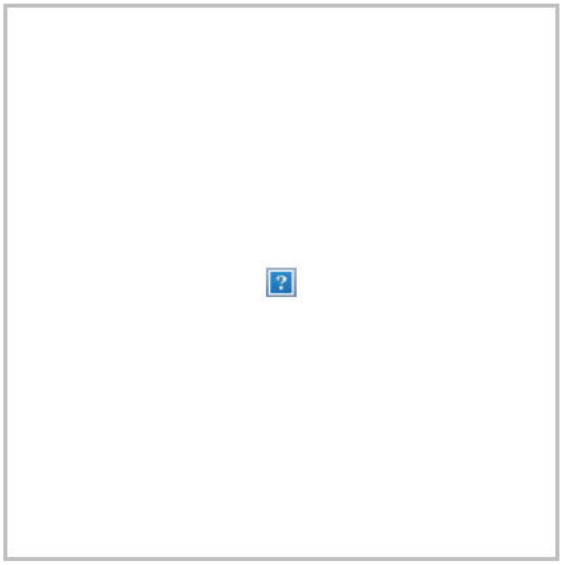


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



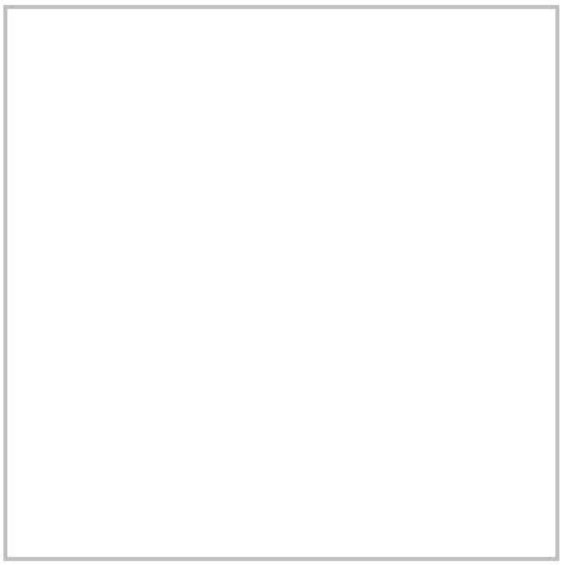
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

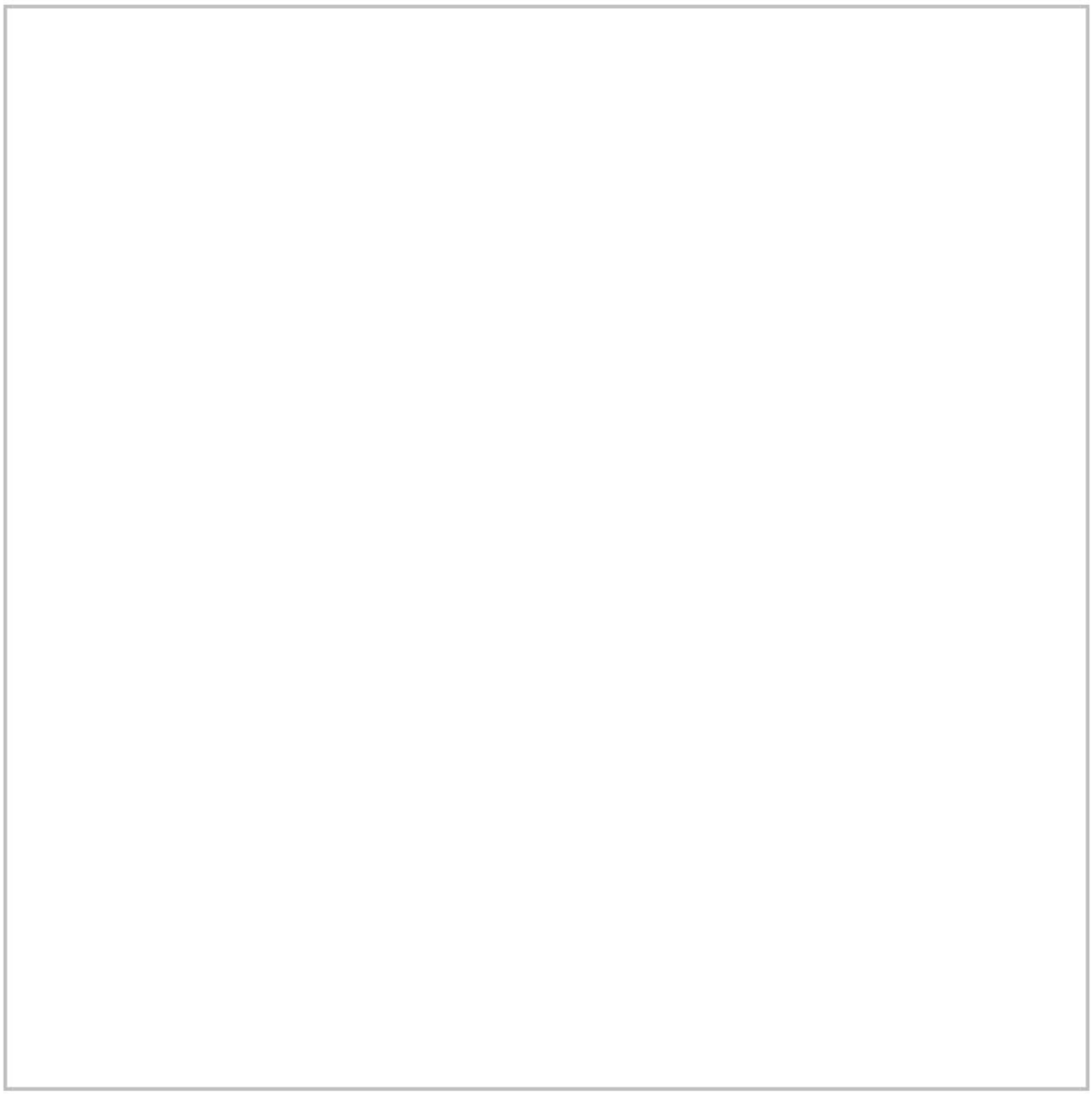
The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE



Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.



Let's Talk Holsters

When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

Integrating Technology: Juggling Public Safety Mission with High-Tech



2023 Uniform Trends

What law enforcement agencies are buying and what new products to watch.

Going Digital: Harnessing Digital Forensics Technology

The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.

As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION

Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us

This email is being sent to thomas.bakey@pol.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: Walsh, Stephen C (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:03:32 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.

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

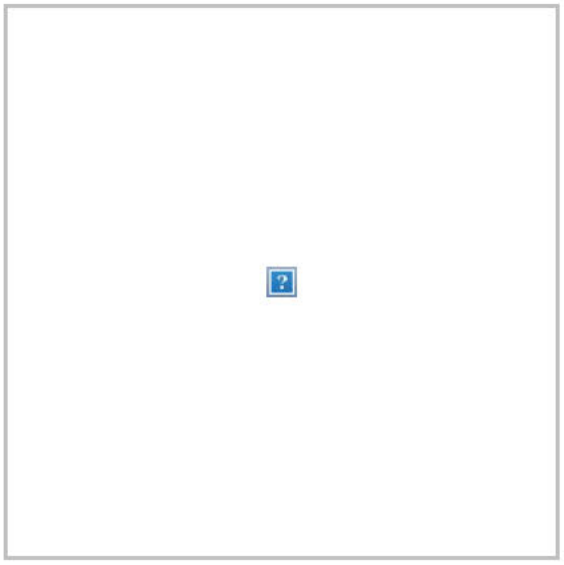
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

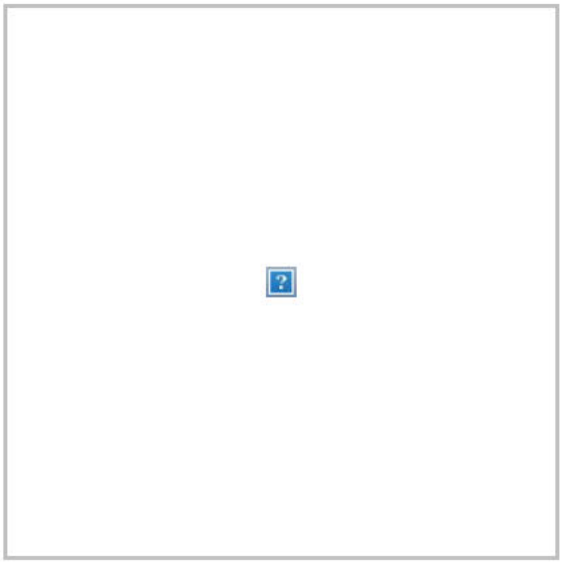
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



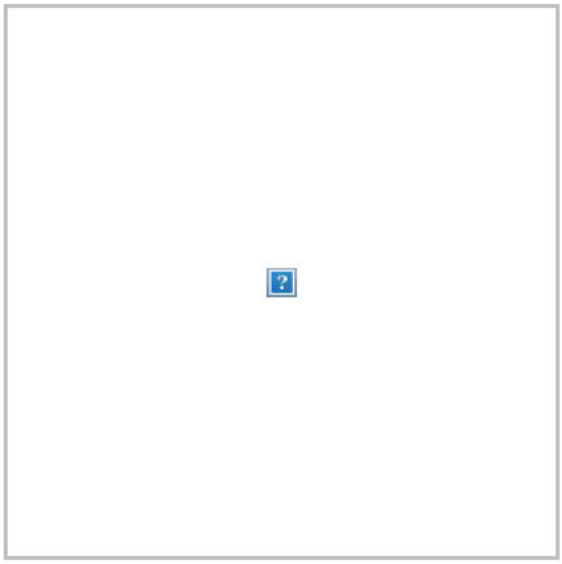
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



V-VICTA

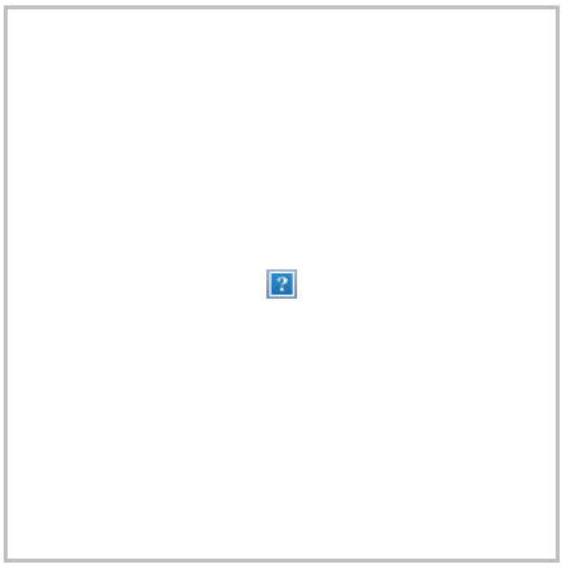
One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

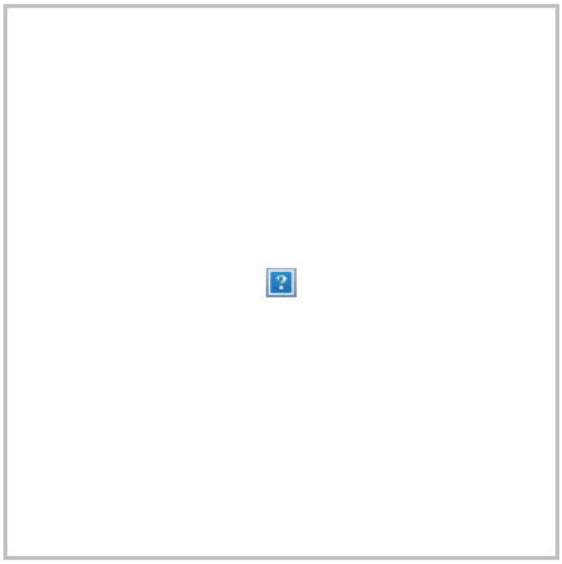
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...

NEW PRODUCTS



Flock Safety Raven

The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem

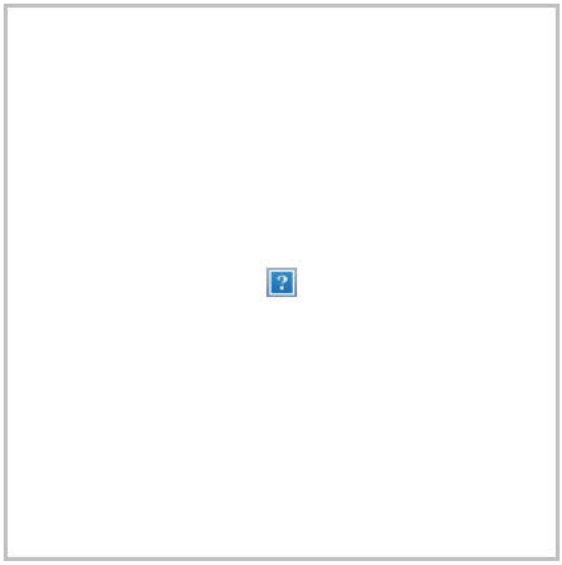


Setina Rear Cargo Storage Box

Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

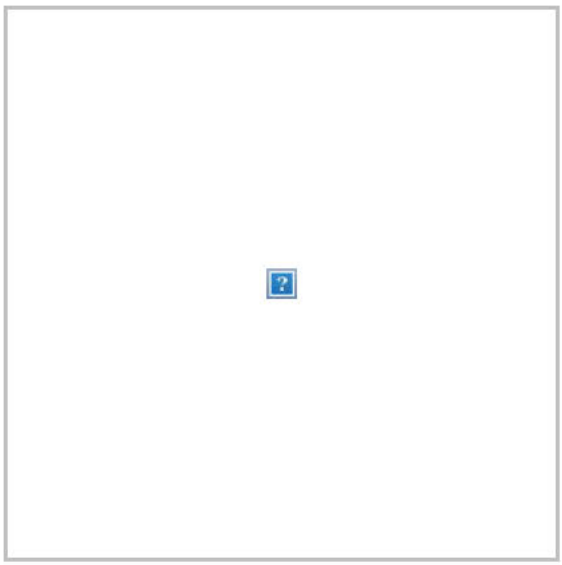


with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

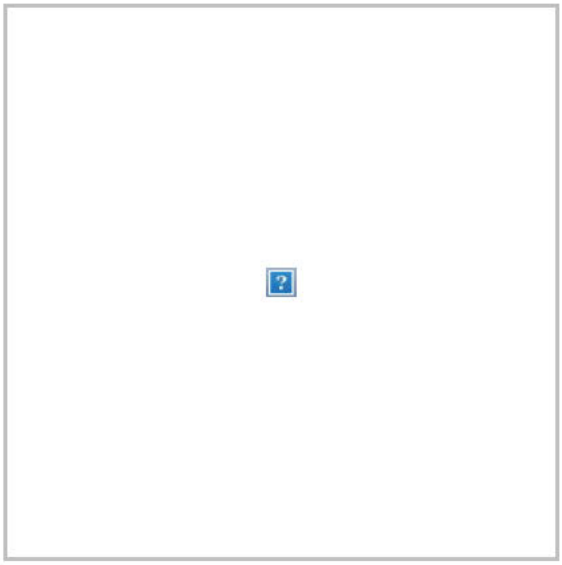


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



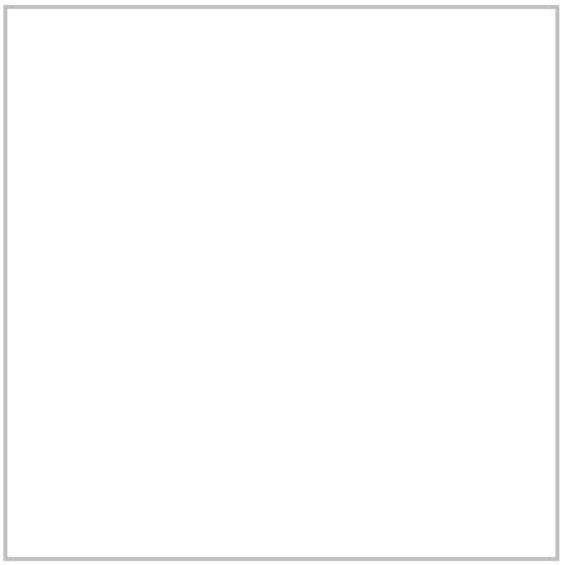
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

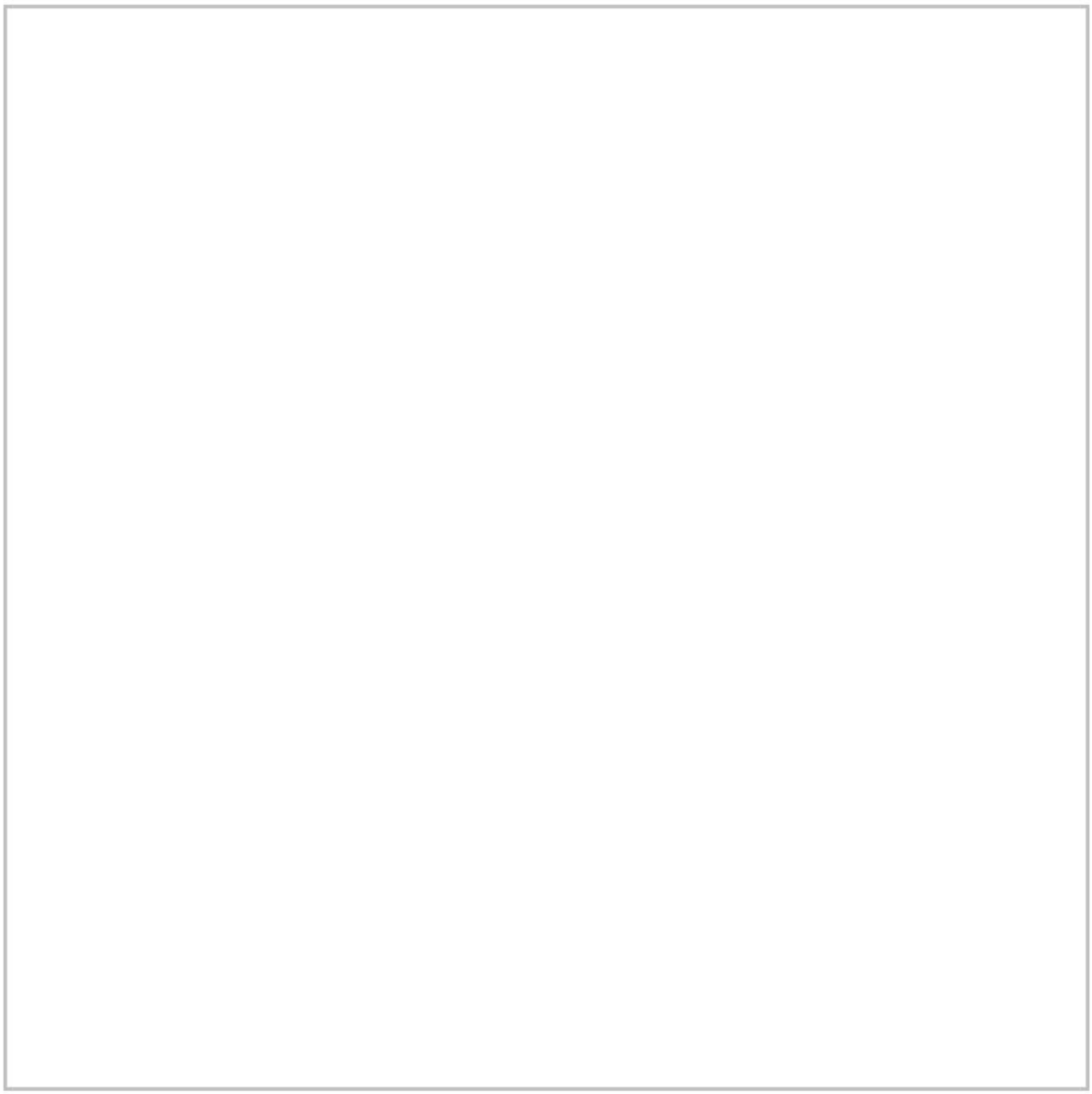
The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE



Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.



Let's Talk Holsters

When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

Integrating Technology: Juggling Public Safety Mission with High-Tech



2023 Uniform Trends

What law enforcement agencies are buying and what new products to watch.

Going Digital: Harnessing Digital Forensics Technology

The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.

As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION

Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us

This email is being sent to stephen.walsh@pol.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: Hanbury, Jason (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:02:03 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.

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

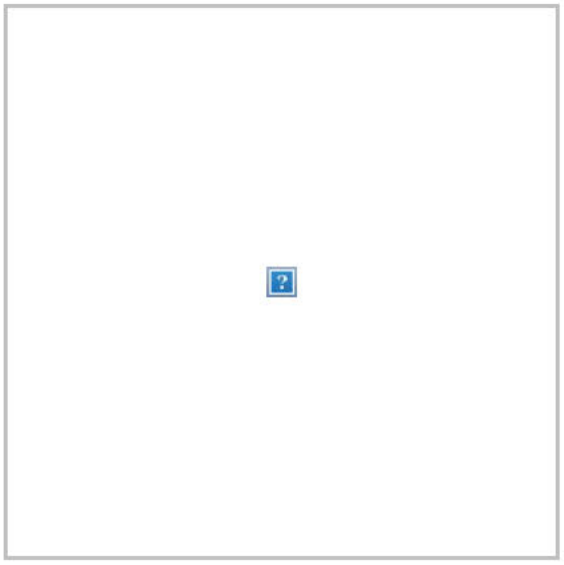
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

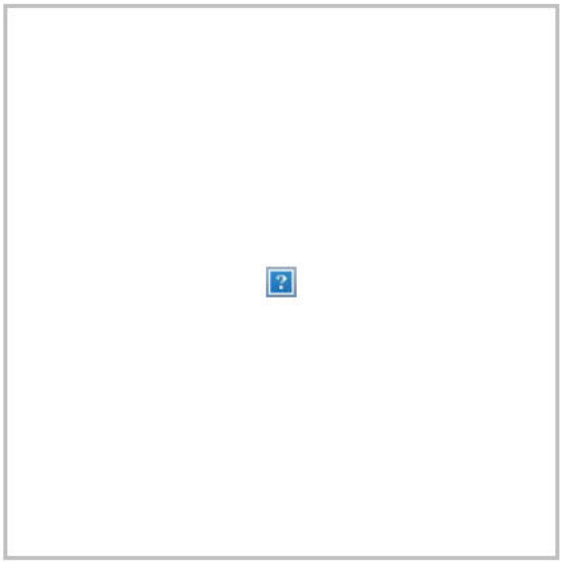
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



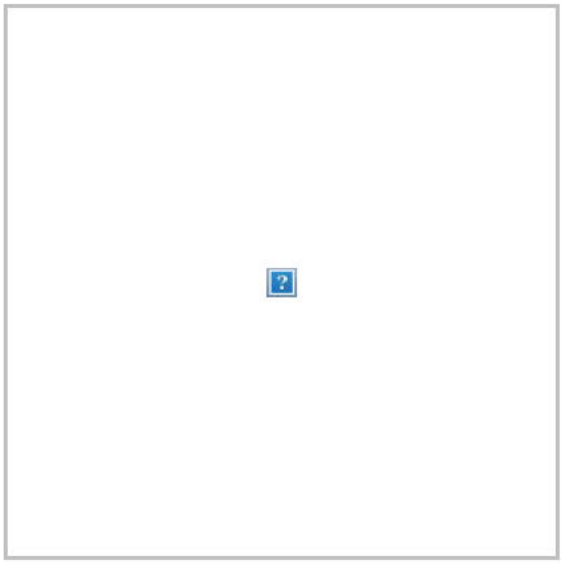
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



V-VICTA

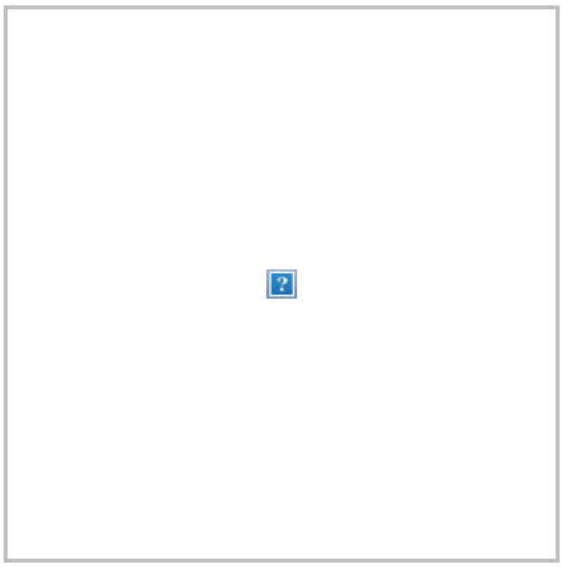
One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

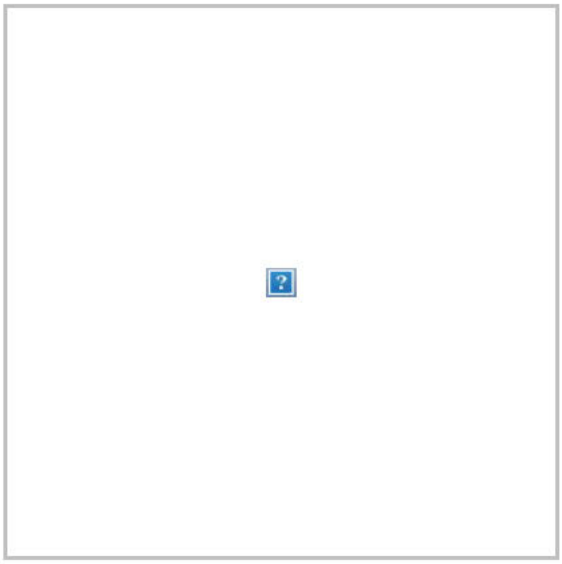
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...

NEW PRODUCTS



Flock Safety Raven

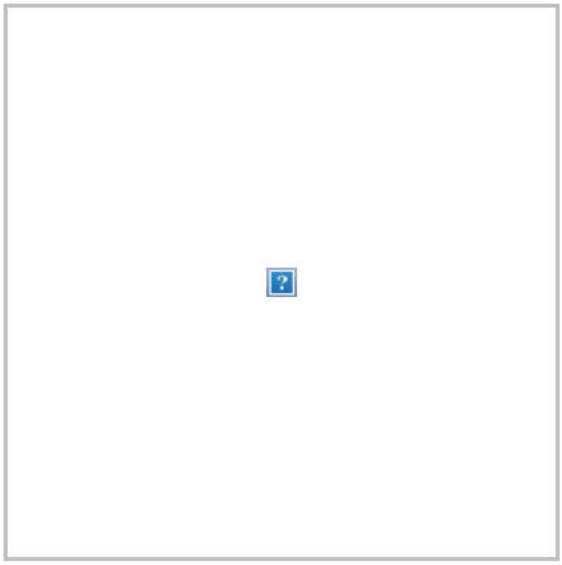
The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem



Setina Rear Cargo Storage Box

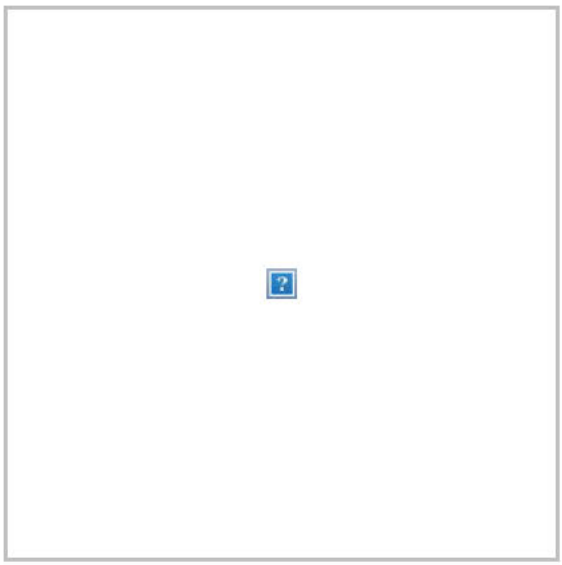
Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

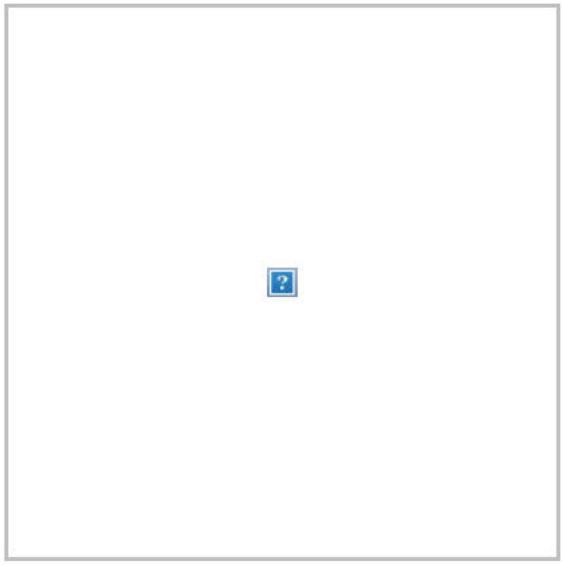


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



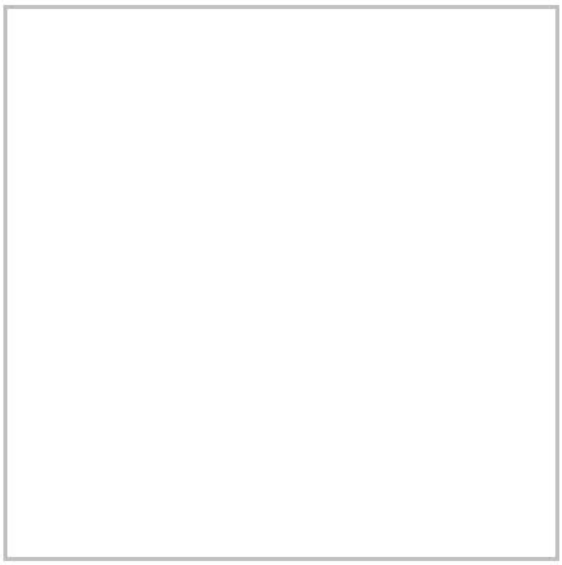
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

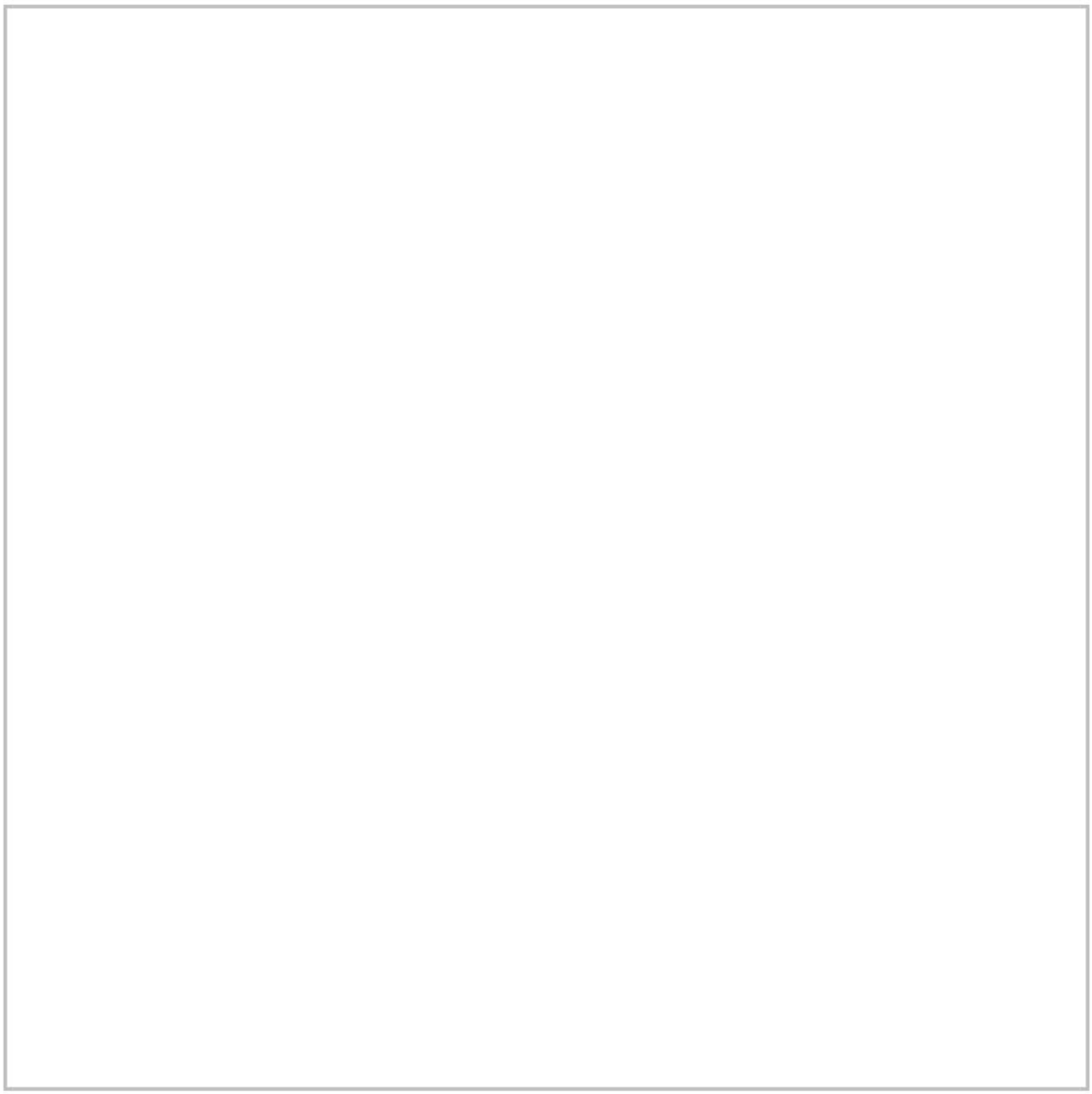
The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE



Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.



Let's Talk Holsters

When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

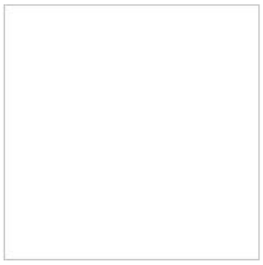
Integrating Technology: Juggling Public Safety Mission with High-Tech



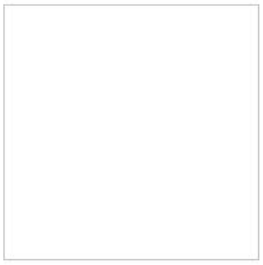
2023 Uniform Trends

What law enforcement agencies are buying and what new products to watch.

Going Digital: Harnessing Digital Forensics Technology

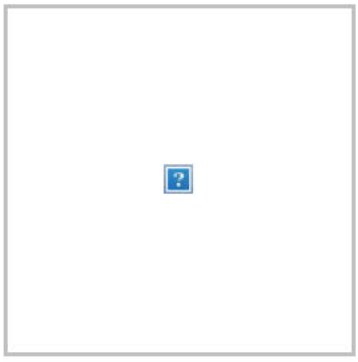


The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.



As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION



Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us



This email is being sent to jason.hanbury@pol.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: O"Brien, Barry (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:01:22 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.

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

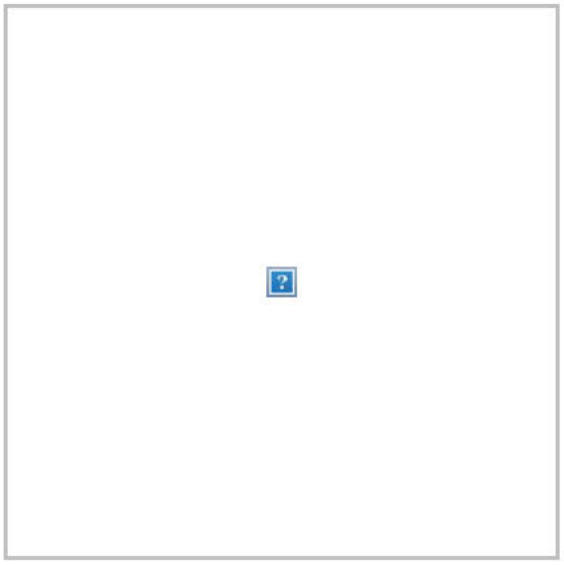
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

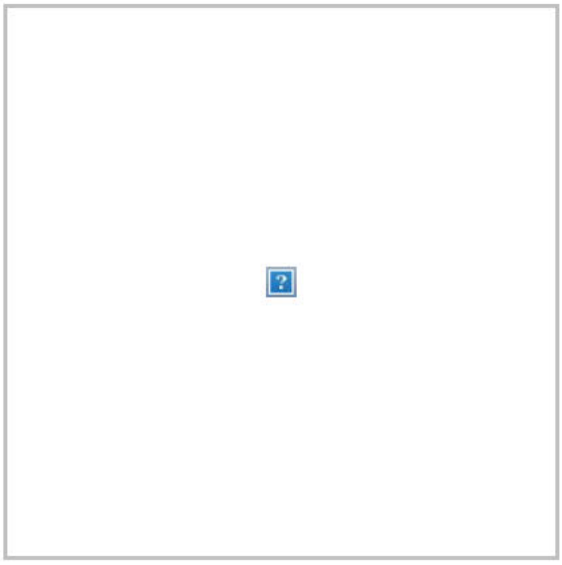
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



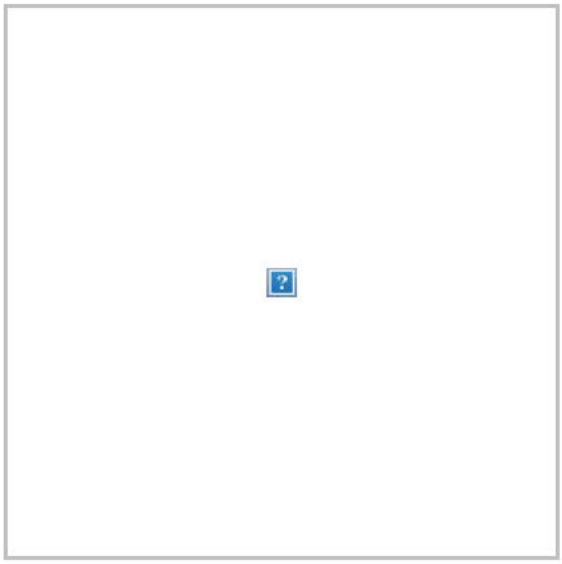
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



V-VICTA

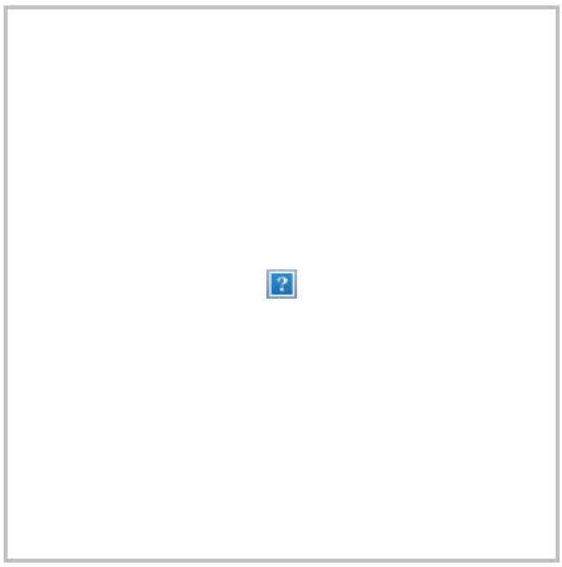
One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

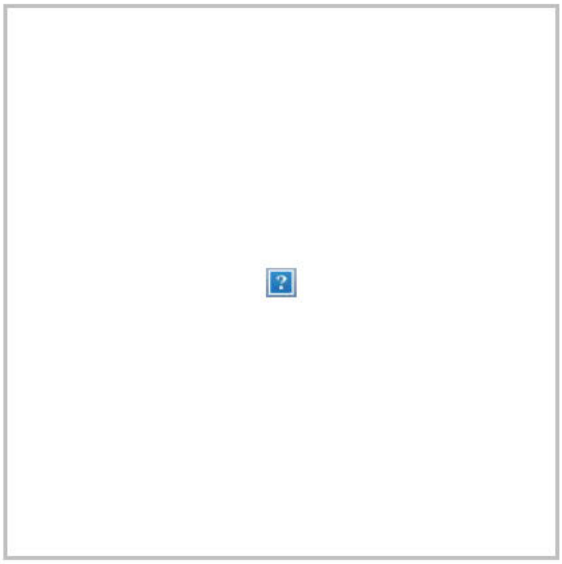
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...

NEW PRODUCTS



Flock Safety Raven

The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem

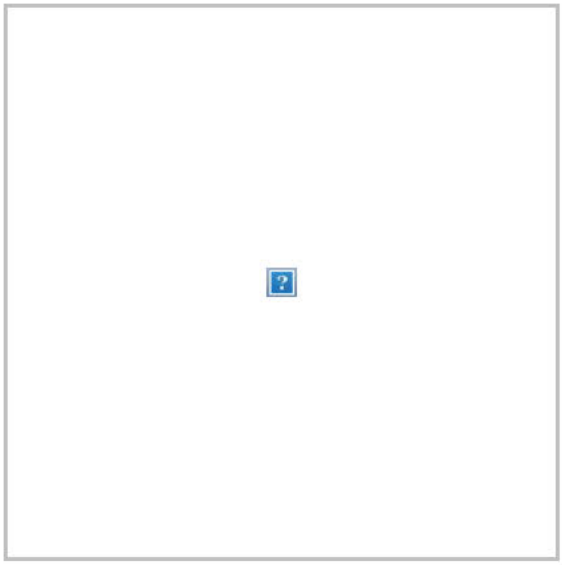


Setina Rear Cargo Storage Box

Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

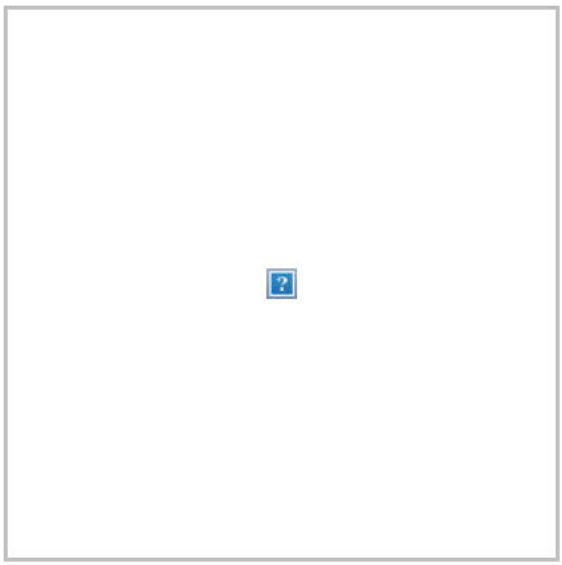


with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

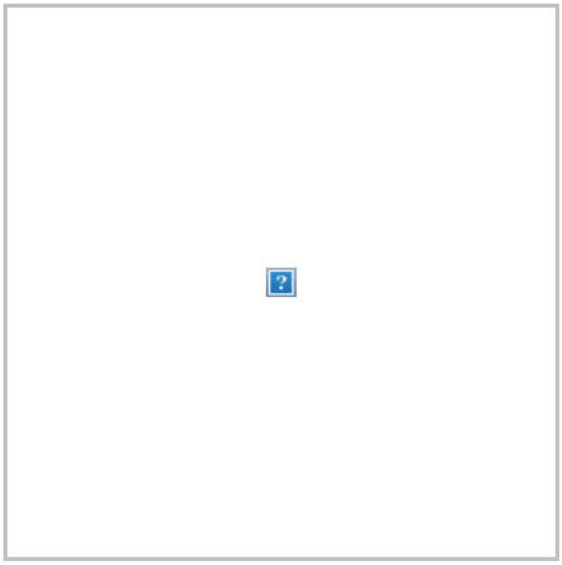


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



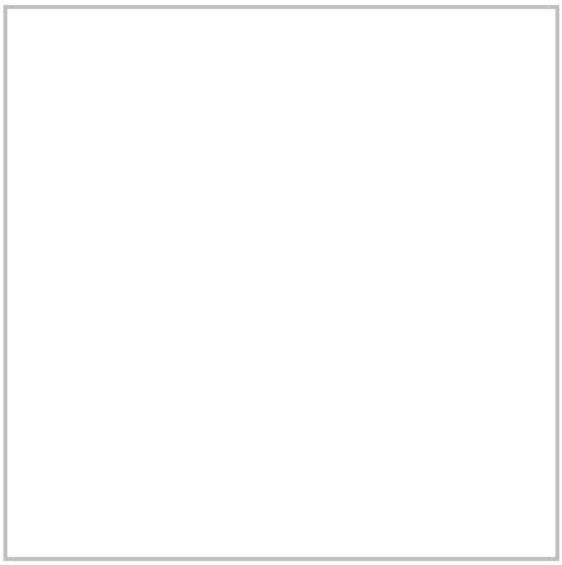
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

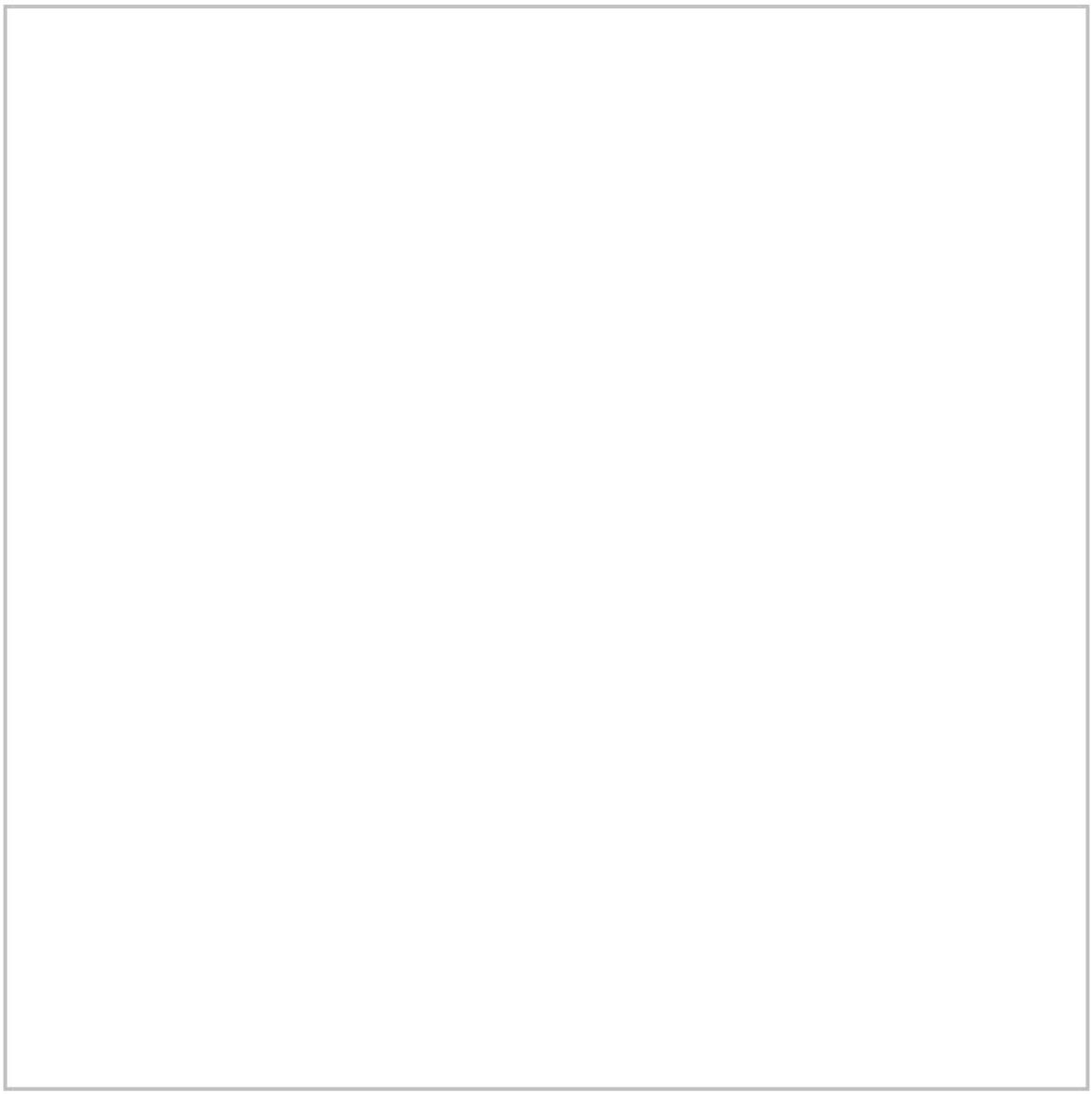
The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE



Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.



Let's Talk Holsters

When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

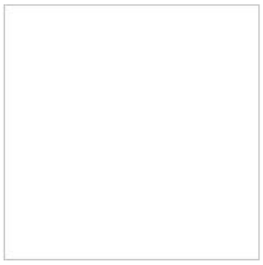
Integrating Technology: Juggling Public Safety Mission with High-Tech



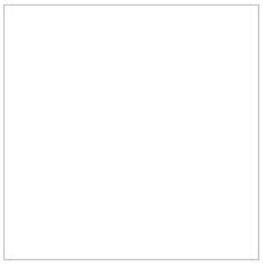
2023 Uniform Trends

What law enforcement agencies are buying and what new products to watch.

Going Digital: Harnessing Digital Forensics Technology

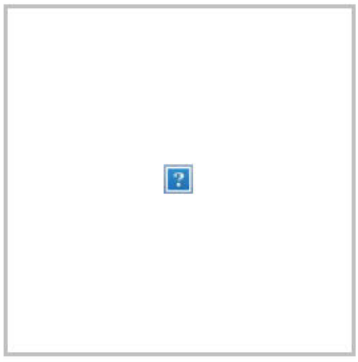


The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.



As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION



Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us



This email is being sent to barry.obrien@massmail.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: OFFICER Magazine
To: zzRizos, Byron (POL)
Subject: Guardian Series | TELR X4000 | P8X Metal Detector | Firearms & Accessories
Date: Friday, April 28, 2023 12:19:23 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.

Officer Magazine Product Focus eNL | View online

officer.com header logo

April 28, 2023

FEATURED

Guardian Series

The Guardian Series from Point Blank Enterprises features a fully-integrated modular design that offer convenient customization, instant adaptability and a

broad range of options. These design features allow you to specially design a Guardian vest that best meet your individual needs for form, fit and function. Ergonomically engineered to allow maximum...



TELR X4000 Light Bearing Holster

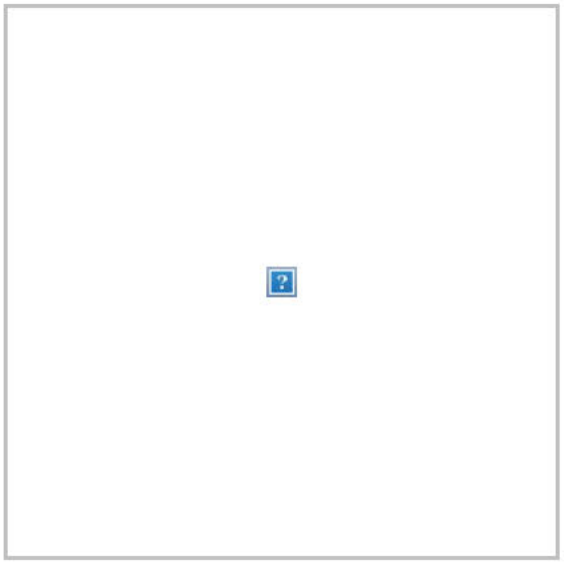
The TELR Level 3 Duty Holster from Gould & Goodrich, a Point Blank Enterprises company, provides the security officers need with the speed they demand. Fits available for Glock 19, 17, 45, 20, 21 and Sig Sauer P320 Compact, Full Size, and X5 with Streamlight TLR 1, Surefire X300 and similar lights.The thumb-activated hood and ejection port releases...



P8X Metal Detector

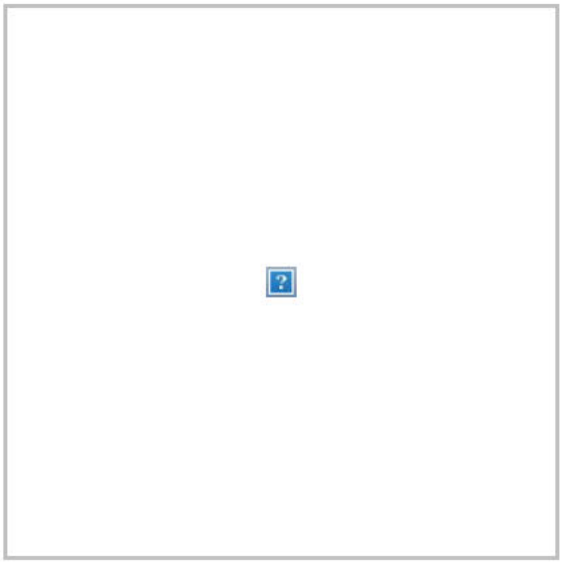
With a 200 foot depth rated housing and a 6 foot maximum detection range, the Pulse 8X from JW Fishers is the company's top of the line detector. It's heavy duty construction and high sensitivity make the Pulse 8X the choice of professionals everywhere. This commercial-grade metal detector is used by law enforcement agencies and military units worldwide...

EDITOR'S PICKS



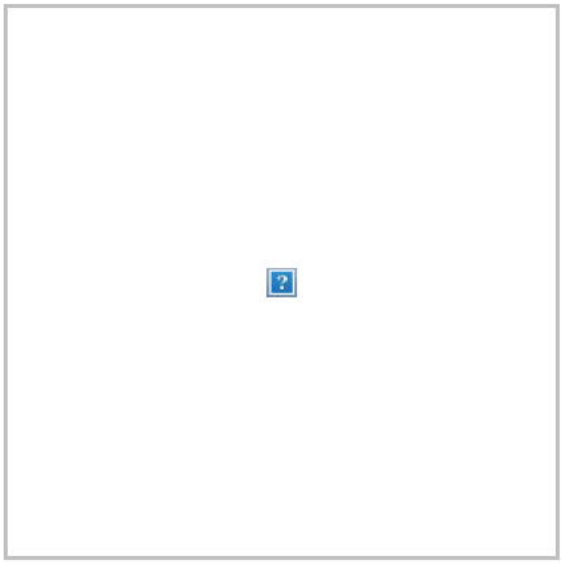
ELSAG Street Sentry

Leonardo's ELSAG Street Sentry is a fixed ALPR that economically aids law enforcement with real-time vehicle interdiction and investigations.It is an autonomous system meaning it has its own power source included, both solar and battery. Agencies will find suspect vehicles faster with a single deployment of the ELSAG Street Sentry. Its low cost also...



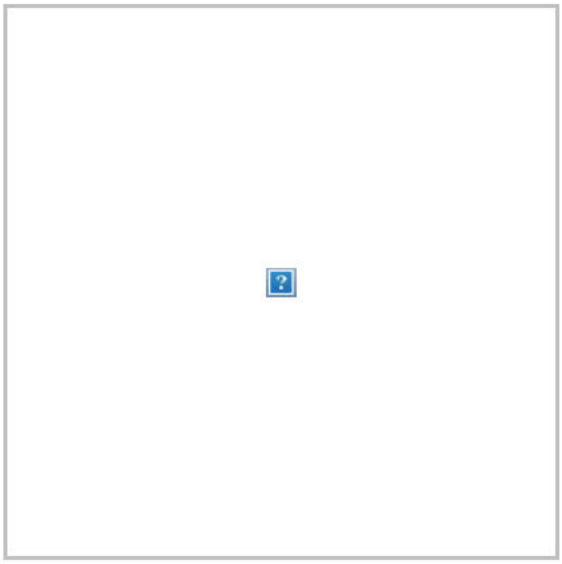
V-VICTA

One of the most important aspects of law enforcement simulation training is the quality of the content. VirTra's V-VICTA—Virtual Interactive Coursework Training Academy—delivers the only nationally certified simulation curriculum for law enforcement training. The curriculum is developed exclusively with nationally recognized partnerships and is designed...



Docking Station for PANASONIC Toughbook 40

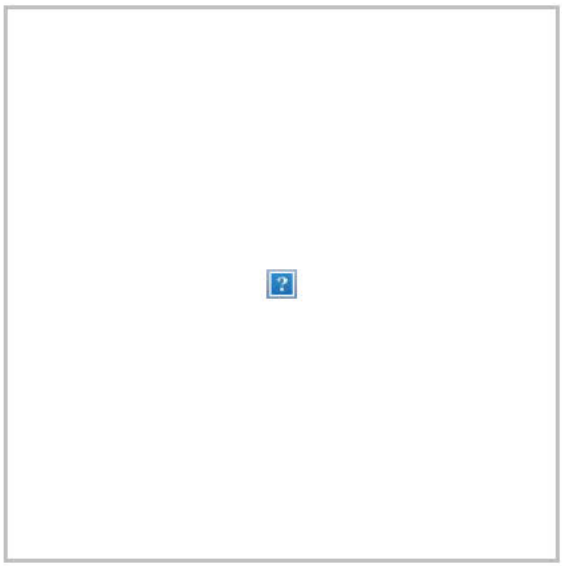
Gamber-Johnson is excited to announce our new docking solution for the Panasonic Toughbook 40 rugged laptop. This docking station features full and lite port replication options including HDMI (full port replication), Ethernet, Serial, USB-A, USB-C, and USB-C with DisplayPort.Your fleet will experience full productivity on the go with Panasonic Toughbook...



Setina Rear Cargo Storage Box

Setina's Rear Cargo Storage Box is available in multiple tiers and configurations to meet any department's needs. The top tier is available with any Setina lock option, including the new keyless RFID or KEY PAD locking systems. The lower slide out equipment tray tier is designed with 300 lb. capacity, lock-in, lock-out Accuride slide rails. An optional...

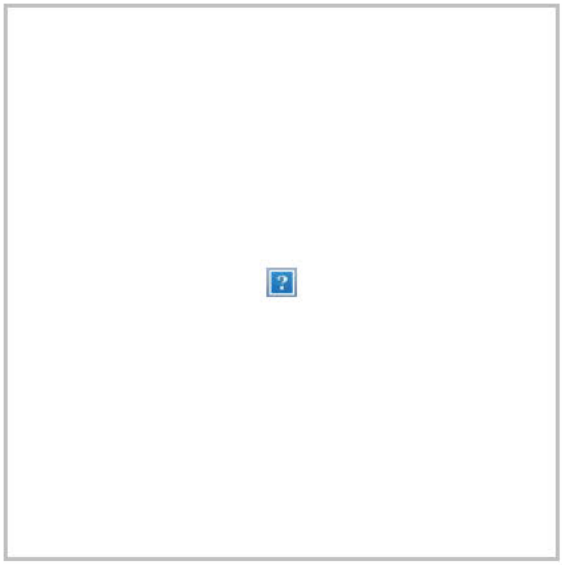
NEW PRODUCTS



Flock Safety Raven

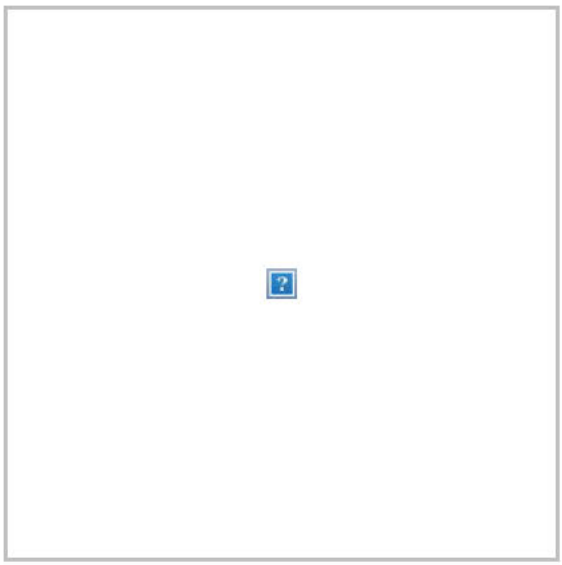
The Raven from Flock Safety is an audio detection device that detects gunshots, locates the source, and works in tandem

with the Flock Safety Falcon ™ Automatic License Plate Reader (ALPR) camera to deliver the objective evidence officers need to respond to gunshots quickly, preserve critical evidence, and clear more cases.Raven recognizes gunshots...

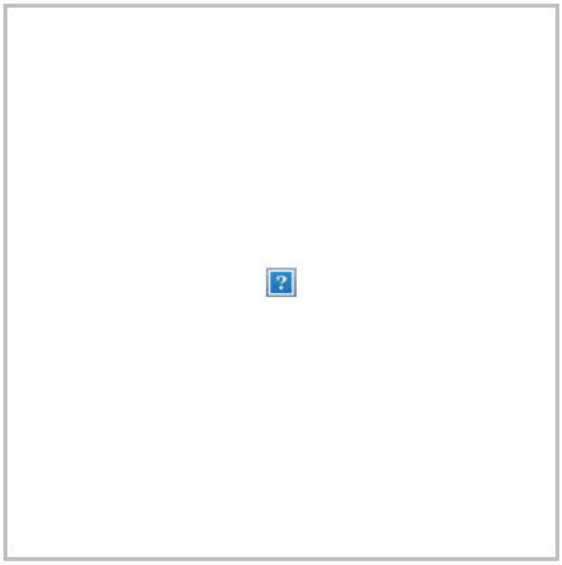


Dyneema

As the world's strongest fiber™, Dyneema® is 15x stronger than steel yet light enough to float on water. In soft armor vests, Dyneema® is up to 35% lighter than aramids. In hard armor plates and inserts Dyneema® is up to 75% lighter than steel and 25% lighter than aramids. As the only backwards integrated ultrahigh-molecular-weight polyethylene (UHMWPE...



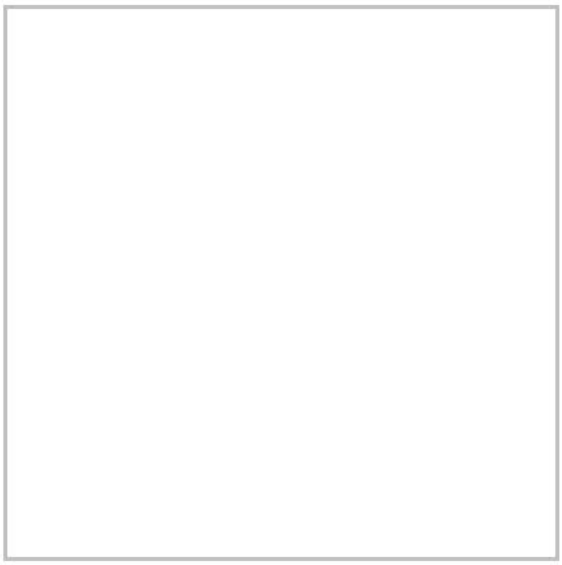
SF-M4 Training Rifle



Magnet AUTOMATE: Keep Investigations Moving 24 Hours a Day, 7 Days a Week, 365 Days a Year

Magnet AUTOMATE by Magnet Forensics Inc. is a forensic evidence automation solution that allows police agencies to keep digital investigations running 24 hours a day, seven days a week, 365 days a year without the need for human intervention.Digital evidence is accumulating at a rate that most police agencies cannot handle, leading to months-long backlogs...

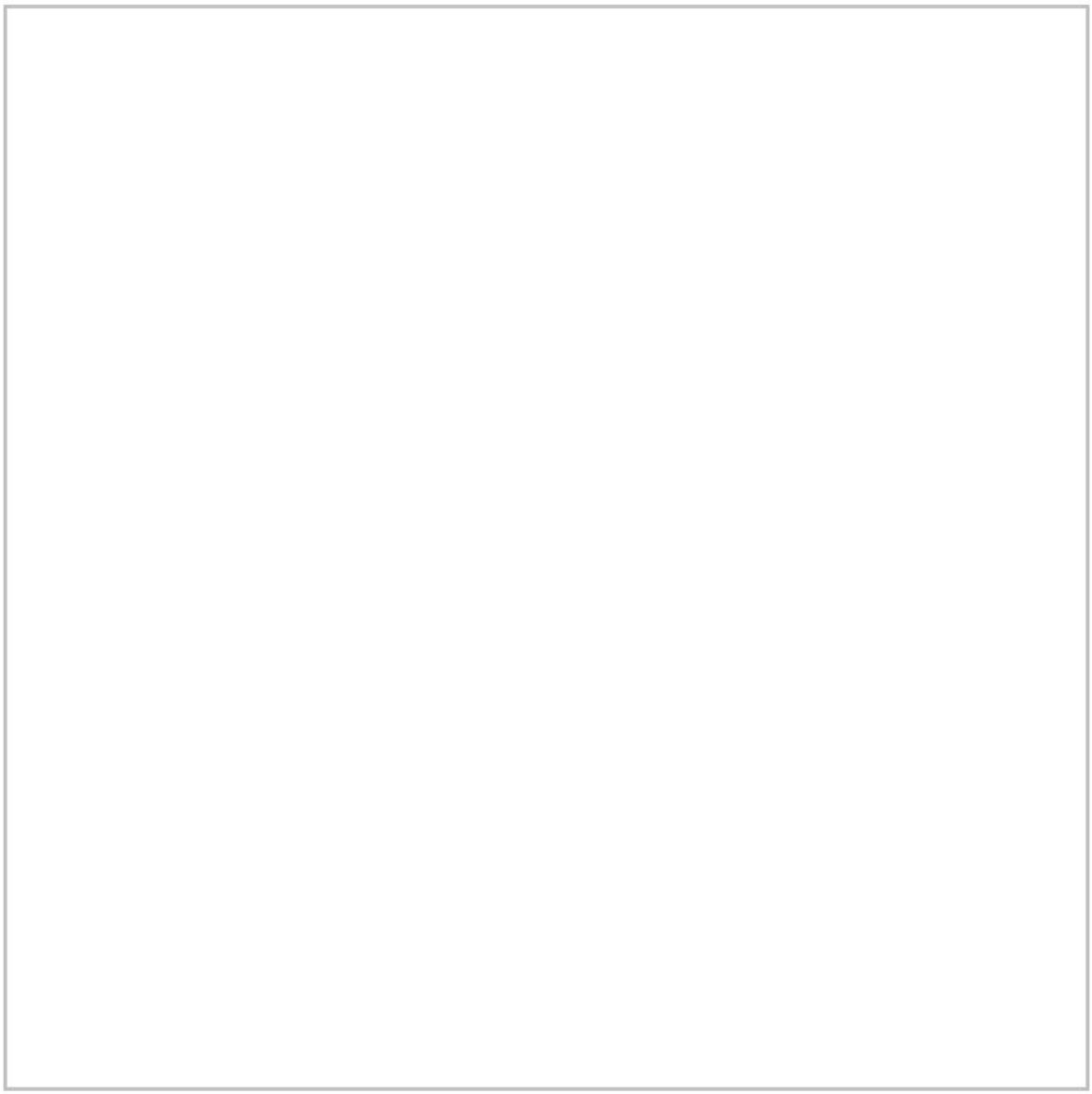
The Smart Firearms SF-M4 Training Rifle is a revolutionary training device with features never before seen on any other style training gun. The new cast aluminum M-4 training rifle with a wide array of features never before seen on any competitive training product for the M-4 rifle. The state-of-the-art, new training product is the closest yet to a...



CentralSquare Unify

CentralSquare Unify offers cross-jurisdictional glue to connect public safety agencies to one another when a crisis strikes. Through our patented and deployed technology, dispatch centers can communicate seamlessly via a full bi-directional data-sharing network, to send the best, most appropriate unit to any call, regardless of jurisdictional boundaries...

IN THIS ISSUE



Beretta APX A1 Review

The Beretta APX A1 is a striker-fired handgun chambered for 9mm and with a standard magazine capacity of 17 rounds. Find out what OFFICER Magazine's test team thought of the weapon.



Let's Talk Holsters

When it comes to carrying your chosen defensive handgun, how and where on your body are obvious considerations.

Integrating Technology: Juggling Public Safety Mission with High-Tech



2023 Uniform Trends

What law enforcement agencies are buying and what new products to watch.

Going Digital: Harnessing Digital Forensics Technology

The evolution of technology has brought both solutions and challenges as police departments and law enforcement agencies try to strike a balance with a public safety mission.

As the role of digital forensics has grown, so has the need for officers and detectives to become involved in the process.

READ THE LATEST DIGITAL EDITION

Read the Officer Magazine March/April 2023 Digital Edition

© 2023 All rights reserved, Endeavor Business Media, LLC.

Connect With Us

This email is being sent to byron.rizos@pol.state.ma.us.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: How a solo LEO stopped an active shooter; Patrol breaching tools
Date: Monday, May 29, 2023 5:02:08 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.

May 29, 2023 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Welcome to this special edition of the Police1 member newsletter, dedicated to the complex issue of police response to active shooter incidents.

Active shooter incidents are unpredictable and evolve quickly. These high-stress situations require decisive AND rapid responses. Your commitment to ongoing training will help you to react swiftly, reduce casualties, neutralize threats and manage the aftermath more efficiently. Preparation today could make the difference between life and death tomorrow.

In today's newsletter, we explore a variety of approaches, tools and training utilized by police departments across the nation and share an inspiring story of a Massachusetts sergeant who single-handedly stopped an active shooter. We also take a retrospective look at several active shooter incidents. Through this analysis, we aim to understand what worked and what didn't, and how we can learn from these events to better prepare our response.

We hope this newsletter provides not only crucial information but also provokes thoughtful discussion. It's through continued dialogue, training and preparedness that we can collectively aim to handle these challenging scenarios more effectively.

Stay safe,

— *The Police1 Team*

PATROL RESPONSE

Breaching tools for every officer

By Philip Paz

The time has come for all law enforcement agencies to greatly expand their breaching tools and related training programs

Ballistic shields can improve officer safety

By Todd Fletcher

It's unacceptable to make patrol officers wait for a supervisor or SWAT



officer for a ballistic shield, so let's properly equip the first officers to arrive on scene



Patrol is SWAT during an active killer event

By Warren Wilson

Officers need to be trained to that level of response – and SWAT officers are the ideal training resource



How a Mass. sergeant singlehandedly stopped an active shooter

By Lt. Dan Marcou

"Train to the point where your training automatically kicks in when the situation starts," says Sergeant Nick Bettano

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

Parallel epidemic: The troubling resurgence of stimulants (white paper)



Increasingly novel combinations of illicit narcotics are deadlier than ever, adding new urgency to combatting the drug crisis.

Download the white paper to learn more

INCIDENT ANALYSIS

Nashville PD's response to the Covenant School active



shooter was 'by the numbers'

By Lt. Dan Marcou

As a trainer, I must state unequivocally that the Nashville officers excelled in their response to this tragedy. And here is how they did this, by the numbers



6 lessons from the Saugus High School shooting

By Mike Wood

The first armed responders to arrive at the shooting were three off-duty officers, a reminder that it's crucial to carry your firearm off duty



Rapid response: The Nova Scotia active shooter incident

By Mike Wood

A highly mobile killer went on a 60-mile, 12-hour spree that ended with 18 killed, including an RCMP constable



Active shooter response considerations: Advice from the front line of the Aurora theatre shooting

By Scott Burhmaster

The incident was not only deadly, it was also tactically eye-opening

Grant assistance for License Plate Readers at no cost



Neology has partnered with PoliceGrantsHelp to provide customized grant help for License Plate Readers, including grant research, alert notices and application reviews.

Get Started Today

Grants funding opportunities for your agency



Join us to learn the best practices in researching and applying for grants.

Register for the webinar - Wednesday, June 7 (1 pm ET)

TRAINING TIPS



"SLED" lead trainer answers 10 questions about active shooter response

By Lt. Dan Marcou

"Through high-quality, repetitive training, we will become a safer country."



Lessons learned from 7 years of active shooter response training

By Major Rich Kuong and Colonel Richard L. Herrington

LEOs must develop fundamental knowledge and skills in tactical operations to credibly address horrific active shooter incidents



7 common active shooter training mistakes

By Jim Morrissey

Great active shooter incident training takes a concerted effort to make exercises real, relevant, interesting and captivating for all participants



Virtual tabletop exercise: Public safety leaders demonstrate importance of interagency training

By Greg Friese, MS, NRP

From "armadillos to zombies," unified command tabletop exercises prepare public safety personnel for real-life mass casualty incidents

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 © 2023 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Pack, Noah (POL)
To: Cyr, Mark (POL)
Subject: Language Draft
Date: Thursday, March 2, 2023 11:09:41 AM

Sir, this is what I had in a draft (it is in the one I sent a few weeks ago) but was not in the one I sent them yesterday:

The Massachusetts Supreme Judicial Court has recognized that individuals have a reasonable expectation of privacy in the whole of their public movements (see *Commonwealth vs. McCarthy, 484 Mass. 493*). While the SJC indicated that the limited use of ALPR does not infringe upon a constitutional right, and therefore does not require a search warrant or other legal process, the widespread and long-term use of ALPR to investigate an individual may amount to a constitutional violation.

Combining this with their suggestions, it could look like:

The Massachusetts Supreme Judicial Court has recognized that individuals have a reasonable expectation of privacy in the whole of their public movements (see *Commonwealth vs. McCarthy, 484 Mass. 493*). While the SJC indicated that the limited use of ALPR does not infringe upon a constitutional right, and therefore does not require legal process, the extensive or long-term use of ALPR in active criminal investigations that do not involve exigent circumstances should be reviewed with a prosecutor of jurisdiction in the investigation for review of the potential necessity of a search warrant.

I'll review McCarthy again for other thoughts.

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: Arunima Choudhary
To: Foley, Kristine (POL)
Subject: Let"s connect to discuss our GeoShield RTCC Solution.
Date: Monday, May 22, 2023 11:20:19 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.

Dear Kristine,

Hope this email finds you well.

I have been attempting to contact you several times in the past especially in my last mail on 3rd May'23 which elaborated our GeoShield RTCC Solution:

1. Uniquely connects multiple data sources like CAD, RMS, AVL, ALPR, etc.
2. Re-Designed Dashboard for Immersive Experience & Quick Access.
3. City Monitoring and Situational Awareness.
4. Advanced Mapping and Spatial Analytics.

My purpose in reaching out to you today is to inquire whether you anticipate a need for the RTCC Solution mentioned above within the next two years.

Would like to offer our assistance by providing you a one-on-one interactive session with our experts to give you a better understanding of the potential scope of the Real-Time Crime Center initiatives for 2023-2024.

To facilitate this, would propose scheduling a call at a mutually convenient time.

Look forward to hearing from you soon.

Thank you.

Cheers,
Arunima Choudhary
(630) 214 – 9787
arunima.choudhary@spatialitics.com

From: Arunima Choudhary
To: Wilczynski, Kristin (POL)
Subject: Let"s connect to discuss our GeoShield RTCC Solution.
Date: Monday, May 22, 2023 11:21:05 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.

Dear Kristin,

Hope this email finds you well.

I have been attempting to contact you several times in the past especially in my last mail on 3rd May'23 which elaborated our GeoShield RTCC Solution:

1. Uniquely connects multiple data sources like CAD, RMS, AVL, ALPR, etc.
2. Re-Designed Dashboard for Immersive Experience & Quick Access.
3. City Monitoring and Situational Awareness.
4. Advanced Mapping and Spatial Analytics.

My purpose in reaching out to you today is to inquire whether you anticipate a need for the RTCC Solution mentioned above within the next two years.

Would like to offer our assistance by providing you a one-on-one interactive session with our experts to give you a better understanding of the potential scope of the Real-Time Crime Center initiatives for 2023-2024.

To facilitate this, would propose scheduling a call at a mutually convenient time.

Look forward to hearing from you soon.

Thank you.

Cheers,
Arunima Choudhary
(630) 214 – 9787
arunima.choudhary@spatialitics.com

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Man with hidden gun opens fire on police in back seat of cruiser
Date: Monday, March 13, 2023 3:55:57 PM

March 13, 2023 | View as webpage | Too many emails? Update Subscription Preferences

TOP STORIES

Mo. officer fatally shot, another wounded by man at gas station

Detective Sgt. Mason Griffith was killed and another officer remains in serious, but stable condition

Man opens fire on Calif. police from back seat of patrol vehicle

Video: Interim Phoenix chief speaks on increase of officer-involved shootings

Broken, dysfunctional and horrible: Kansas officers describe culture in report

San Diego police chief calls for repeal of loitering law to help fight sex trafficking

Video: Ore. murder suspect captured after escaping from courthouse

FEATURED CONTENT



How to build and sustain an effective officer wellness program: A Policing Matters Special

By Police1 Staff

Learn how the Stanislaus County Sheriff's Office's built an award-winning holistic officer wellness program



Skipping an easy step leads to suppression

By Ken Wallentine

This case illustrates how good police work can easily be marred by failing to secure a warrant

How to buy body-worn cameras (eBook)



Download this Police1 body-worn camera buying guide to learn key steps for product selection, purchasing and implementation.

Download now

FAMILY & HOME

Making choices for elder care

By Missy Morris

Regardless of what option turns out to best fit your family's needs, there are some very important points to remember as you're making choices

Basic estate planning for first responders

By Lynzie Wolters

Regardless of your level of wealth, the failure to establish an estate plan can be detrimental to your family

SPONSORED CONTENT

Why Neology is an ALPR partner you can rely on

Police departments need an ALPR like the Neology Helios, which features powerful on-camera processing that provides immediate results.

FEATURED JOB

Work where everyone wants to live!
Apply Now!

FEATURED RESOURCES

Grant assistance for Officer Wellness products at no cost
Customized grant help from Cordico for officer wellness products, including grant research, alert notices and application reviews.

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 © 2023 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: FINDER Events
To: zzEgnitz, Brian (POL)
Subject: No Time for Downtime. Register for our webinar today!
Date: Thursday, June 8, 2023 11:05:59 AM

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

View in browser

weBINAR

What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to data.

FINDER Virtual Technician (FVT) is a web-based application that allows system

administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have CCTV, fixed or trailer-mounted LPR systems, FVT monitors the key hardware components of your security intelligence portfolio.

Join us as we discuss the following:

- A look at technology and the importance in policing
- Overview of real-life incidents and how FVT could and has assisted.
- Demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

Don't miss this opportunity to leverage the power of FINDER Virtual Technician and revolutionize your agency's approach to system health monitoring.

REGISTER NOW

FINDER® Software Solutions, 11315 Corporate Blvd, Ste 110, Orlando, FL 32817, United States
Unsubscribe Manage preferences

From: FINDER Events
To: Clement, Michael (POL)
Subject: No Time for Downtime. Register for our webinar today!
Date: Thursday, June 8, 2023 11:06:54 AM

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

View in browser

weBINAR



What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to data.

FINDER Virtual Technician (FVT) is a web-based application that allows system

administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have CCTV, fixed or trailer-mounted LPR systems, FVT monitors the key hardware components of your security intelligence portfolio.

Join us as we discuss the following:

- A look at technology and the importance in policing
- Overview of real-life incidents and how FVT could and has assisted.
- Demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

Don't miss this opportunity to leverage the power of FINDER Virtual Technician and revolutionize your agency's approach to system health monitoring.

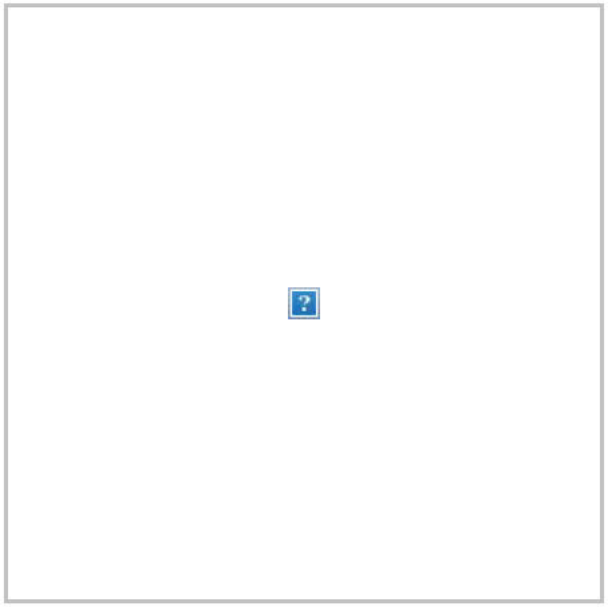
REGISTER NOW

FINDER® Software Solutions, 11315 Corporate Blvd, Ste 110, Orlando, FL 32817, United States
Unsubscribe Manage preferences

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Off-duty NYPD cop shot in head; 6th Memphis officer fired
Date: Monday, February 6, 2023 1:24:15 PM

February 6, 2023 | View as webpage | Too many emails? Update Subscription Preferences

TOP STORIES



Off-duty NYPD officer shot in head in robbery attempt

"Please keep this officer in your prayers. He is currently fighting for his life," Police Commissioner Keechant Sewell said

6th Memphis officer fired in Tyre Nichols arrest

Anchorage PD's new policy now allows officers to carry naloxone

2 Ind. cops wounded after being shot at point-blank range; suspect dead

Photo: Memphis officer consoles, talks 17-year-old from bridge's edge

Woman hailed a hero for disarming D.C. Metro Station gunman

Introducing the latest addition to the Sentinel Armored Rescue Vehicle family.



The new 2023 Sentinel ARV is now offered based off either the Ford F-550 chassis or the Dodge Ram 5500 chassis. All new Sentinel ARV builds

can be delivered within 180 days.

Click For Grant Assistance and Pricing

FEATURED CONTENT



Uncomfortable questions law enforcement must answer after the death of Tyre Nichols

By Jonathan M. Wender, Ph.D.

To demean policing rather than precisely identify its failures and limitations serves only to undermine progress



How do we stop violent crime through technology?

By Sergeant Dalton Webb

Watch a proactive individual in a real-time crime center actively monitor a location for criminal activity

Tips on how police officers can protect their privacy online



While you can't become completely invisible online, you should strive to become a challenging target. Here's why taking these steps is a

BOSS4 – Managed Service ALPR Solution



Intuitive searching and analytics, including powerful map-based, multi-location, searching capability. Our MANTIS 4-D Vehicle Recognition

worthwhile investment.

Learn more

solution provides rich data mining capabilities to find the vehicles you are looking for.

Discover your options

PEER SUPPORT



Book excerpt: Peer Support Fundamentals: Ask, Listen, Encourage, Follow-up

By Brian Casey

Peer support can decrease the unnecessary suffering of coworkers and give the peer supporter a greater sense of purpose



Troy Anderson on effective peer support following a mass shooting response

By Policing Matters Podcast

"When you are dealing with things like a mass casualty with children, it is going to penetrate your armor."



SPONSORED CONTENT



These newly updated earpieces deliver clearer sound with less maintenance

Officers can enjoy comfort and convenience no matter their environment.



FEATURED JOB



Police Officer - $25,000 Lateral Incentive and $10,000 Entry Level Incentive

$6,001 - $8,041 per month/Officer - Vancouver, Washington

FEATURED JOB



Federal Way, Washington $6,147 - $8,342 monthly

Police Officer - $20,000 Lateral Hiring Incentive



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.

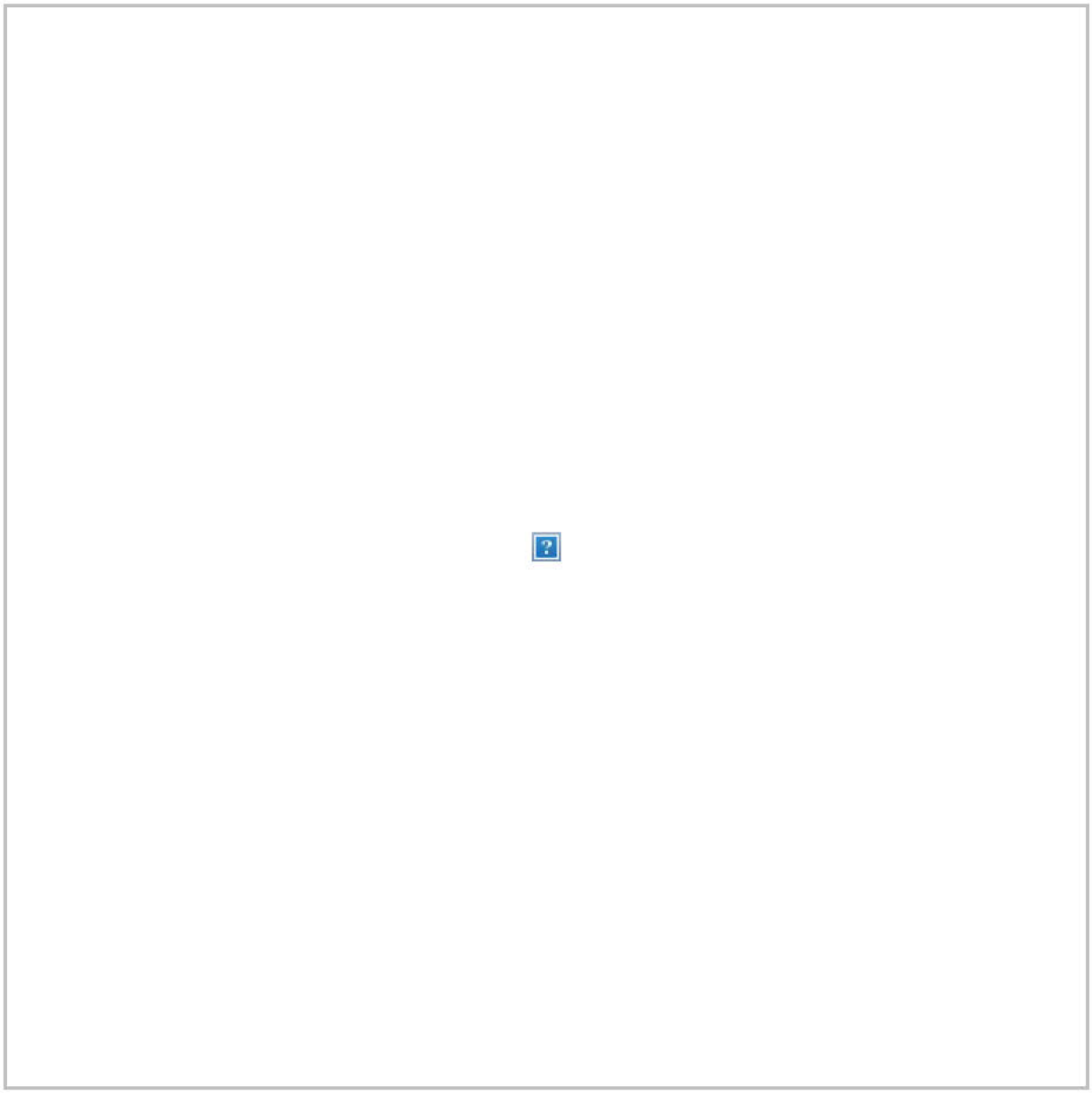
If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2023 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Officer hit by rig at NBA parade could lose leg; SRO ban reversed
Date: Friday, June 16, 2023 3:32:52 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 16, 2023 | View as webpage | Too many emails? Update Subscription Preferences



Officer hit by fire truck at end of parade undergoes surgery to save his leg

During a Nuggets parade, Sgt. Justin Dodge was on the front passenger side of a fire truck protecting fans from traffic when he was caught under the wheels

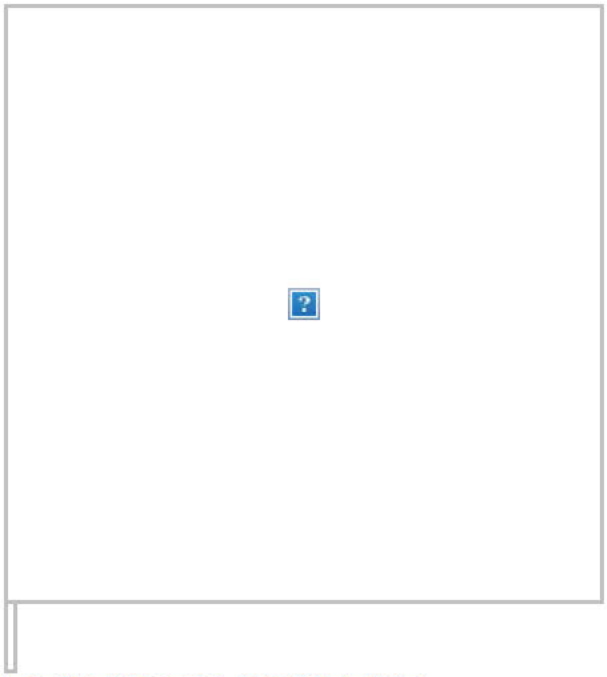
Watch: Pursuit comes to wild end after Texas officers jumped into bayou to rescue toddler

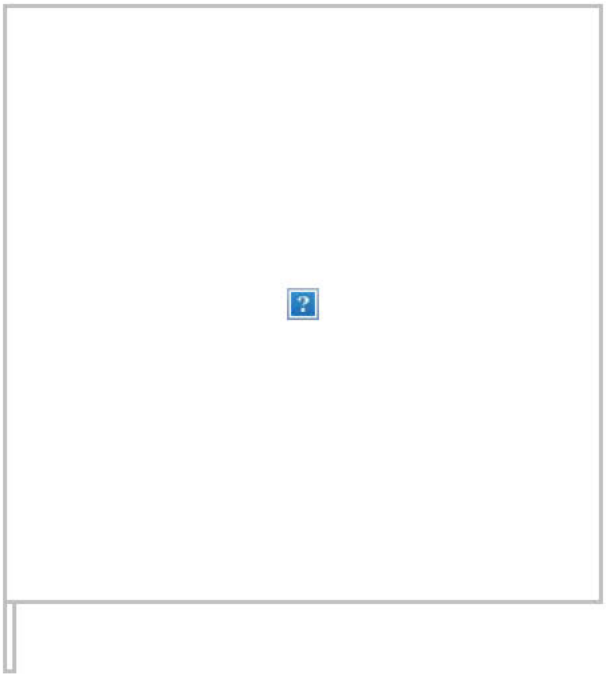
Colo. school board reverses 2020 ban on SROs

Fla. deputy didn't follow extensive training during Parkland school massacre, supervisor testifies

Ga. officer shot in the line of duty returning home nearly a year later

Man charged after shooting his own leg while dreaming about intruder, Ill. deputies say





FEATURED CONTENT

Who is the most influential leader at your agency?

By Leon Reha

Leadership has nothing to do with rank and everything to do with influence

How to become a police lieutenant: Career advice from law enforcement leaders

By Erik Fritsvold, PhD

There are certain universal qualities that have proven successful among law enforcement professionals who have successfully been promoted to lieutenant

What works in retaining and recruiting top-shelf officers



This Minnesota PD is upping its recruitment game by bringing attention to what it does best.

Learn what works

Get closer to Vision Zero.



Schedule a free demo to find out how a total community solution providing speed enforcement, ALPR and video can help change driver behavior and keep communities safer.

Take action today

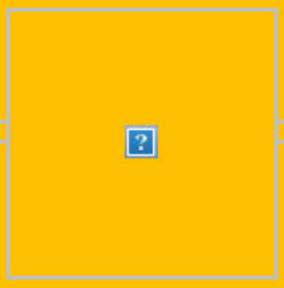


PHOTO OF THE WEEK

To protect and sniff

Albany County police K-9s receive donations of lifesaving Narcan from Protection4Paws

FATHER'S DAY

Father’s Day can be tough for divorced dads

By John G. Weaver

I know the landmines are there, but awareness alone won’t prevent the darkness of depression from creeping in

15 tips from fathers that cops use on patrol

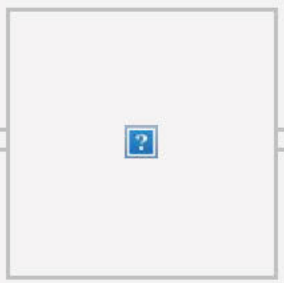
By Police1 Staff

Our readers shared the best advice they’ve received from their dads that they use on the job

Sponsored Content

Survey: Taking the pulse of public safety communications today

Communications technology is vital for first responders. Police1 wants to know how you use these tools on a day-to-day basis. Take our 5-minute survey and enter to win one of four $250 Amazon gift cards!



FEATURED DEAL

5% Discount for Police1 readers

Panasonic Toughbook $399





FEATURED JOB

Alaska State Trooper Entry/Lateral ($10,000 Move Reimbursement)

Anchorage, AK
Entry Level: $37.13 hourly

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 © 2023 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: FINDER Events
To: Clement, Michael (POL)
Subject: One day left to register! Free Webinar: No Time for Downtime.
Date: Wednesday, June 14, 2023 12:24:55 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.

View in browser

weBINAR



What happens when your field hardware devices go down? Whether it's a natural disaster or a system failure, no time is a good time to lose access to data.

FINDER Virtual Technician (FVT) is a web-based application that allows system

administrators and authorized users to view the current status and health of their IP-connected ALPR, surveillance, and communications equipment in the field. Whether you have CCTV, fixed or trailer-mounted LPR systems, FVT monitors the key hardware components of your security intelligence portfolio.

Join us as we discuss the following:

- A look at technology and the importance in policing
- Overview of real-life incidents and how FVT could and has assisted.
- Demonstration of FVT that will show you how to limit field visits with customized monitoring and alerting.

Don't miss this opportunity to leverage the power of FINDER Virtual Technician and revolutionize your agency's approach to system health monitoring.

REGISTER NOW

FINDER® Software Solutions, 11315 Corporate Blvd, Ste 110, Orlando, FL 32817, United States
Unsubscribe Manage preferences

From: ASIS International
To: Upton, Paul (POL)
Subject: Open Forum Digest for Monday April 24, 2023
Date: Tuesday, April 25, 2023 1:15:09 AM

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

Open Forum

Post New Message

Apr 24, 2023

Discussions

started 5 hours ago, Gerald G Wilkins (1 reply)

Active Shooter Preparedness

1. One of the questions I hear most often is, "how... Gerald G Wilkins
2. Dear Gerald, Nicely summed up and certainly... Nishith Agarwal

started 8 hours ago, J Downs (0 replies)

AMAG/Symmetry Latency + Solutions

3. Hello, I was curious if any one else... J Downs

started 10 hours ago, Dwayne M Gulsby (2 replies)

Law enforcement recruitment

4. Police departments are coping with critical... Dwayne M Gulsby
5. Hello Dwayne It's a great question. At the... Kevin Stranahan
6. The situation that you wrote about is further... Brian S Ishikawa

started 2 days ago, David Olmstead (12 replies)

Deterrent value of Cameras at the entrance/exit of a Neighborhood.

7. So I put a lot of those cameras in toll booths... Salvatore A D'Agostino
8. For all ASIS members, Michael's observations on... Felix A Giannini FPE
9. Cameras with out response or action are ... well... Steven J Siegel
10. Message Jeremiah Main
11. David, I spent many years running the... Jeremiah Main
12. Hi David, You've brought up some valid points... Dwayne Cooney

13. I agree with Michael. In today's environment,... Jeffry Queen
14. Hello, I am a security technology... Jon Polly
15. I agree with your points regarding the limited... Nelson Torres

started 4 days ago, James A Cosseboom (5 replies)

Electric Vehicle Fire Mitigation?

16. The UL Fire Safety Research Institute (Home | UL... Al Policano
17. As a member of both NFPA and ICC, I know there... Timothy Diehl

started 4 days ago, Sami Mohammad Daoud Adwan (4 replies)

LED Lighting and CCT

18. Sami, My field of expertise is Perimeter... Matthew Beausoleil

started 5 days ago, Richard P Laib (6 replies)

Training and Development in Video Surveillance Systems

19. NICET Dwayne Cooney

started 7 days ago, Anonymous Member (24 replies)

Photos on access cards, good or bad for security?

20. This message was posted by a user wishing to... Anonymous Member

top next

1. Active Shooter Preparedness

Reply to Group Online | Reply to Sender Online

Apr 24, 2023 7:35 PM
Gerald G Wilkins

One of the questions I hear most often is, "how do I prepare my organization to respond to an All Hazard event:. I believe researching best practice is always a good place to start. FEMA classifies Active Shooter events as ALL Hazard events. So, I summarized the FEMA POETE framework as a potential good place to start.

POETE (Planning, Organization, Equipment, Training, and Exercise) is a framework used in emergency management and disaster response to ensure effective preparedness and response

activities. Here's how you can use POETE:

1. Planning: Develop a comprehensive emergency response plan that outlines the roles and responsibilities of all parties involved in the response effort. ***Identify potential hazards and risks, develop a communications plan, and establish procedures for resource allocation and coordination.***
2. Organization: ***Establish an organizational structure for your emergency response team, including a clear chain of command and designated roles and responsibilities for each member.*** This ensures that everyone knows their role and what they are responsible for during an emergency.
3. Equipment: ***Make sure that all necessary equipment and resources are available and ready for use.*** This includes communication devices, personal protective equipment, medical supplies, and vehicles, among others. Regular maintenance and testing of equipment should also be done to ensure that they are in good working condition.
4. Training: Ensure that all team members have the appropriate training and knowledge required for their roles. ***This includes training on emergency response procedures, the use of equipment, communication protocols, and the identification of potential hazards and risks.***
5. Exercise: ***Conduct regular training exercises to test and evaluate the emergency response plan and identify areas for improvement.*** This ensures that team members are prepared and can work together effectively in an emergency situation.

By utilizing POETE, organizations can better prepare for and respond to emergencies and disasters, ultimately helping to mitigate the impact on people and property.

If you are not sure if you have properly prepared for a All Hazard event at your facility simple take the highlighted statements and pose them as questions to your Security/Risk Management team.
I hope this was helpful!

Jerry G Wilkins, PSP® NREMR® CAHSO® NFPA-3000 Program Specialist
Active Risk Survival, Inc.
Salisbury, Maryland
410-430-1485

View Thread Like Share Discussion Flag as Inappropriate

top previous next

2. Re: Active Shooter Preparedness

Reply to Group Online Reply to Sender Online

Apr 24, 2023 9:23 PM
Nishith Agarwal

Dear Gerald,

Nicely summed up and certainly of a great value..

Regards

[Nishith] [Agarwal] [CPP]
[Raxa Security services Ltd]
[Head Training & Recruitment]
[Military Veteran]
[India]

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 24 Apr, 2023 19:35
From: Gerald G Wilkins
Subject: Active Shooter Preparedness

One of the questions I hear most often is, "how do I prepare my organization to respond to an All Hazard event:. I believe researching best practice is always a good place to start. FEMA classifies Active Shooter events as ALL Hazard events. So, I summarized the FEMA POETE framework as a potential good place to start.

POETE (Planning, Organization, Equipment, Training, and Exercise) is a framework used in emergency management and disaster response to ensure effective preparedness and response activities. Here's how you can use POETE:
1. Planning: Develop a comprehensive emergency response plan that outlines the

roles and responsibilities of all parties involved in the response effort. ***Identify potential hazards and risks, develop a communications plan, and establish procedures for resource allocation and coordination.***
2. Organization: ***Establish an organizational structure for your emergency response team, including a clear chain of command and designated roles and responsibilities for each member.*** This ensures that everyone knows their role and what they are responsible for during an emergency.
3. Equipment: ***Make sure that all necessary equipment and resources are available and ready for use.*** This includes communication devices, personal protective equipment, medical supplies, and vehicles, among others. Regular maintenance and testing of equipment should also be done to ensure that they are in good working condition.
4. Training: Ensure that all team members have the appropriate training and knowledge required for their roles. ***This includes training on emergency response procedures, the use of equipment, communication protocols, and the identification of potential hazards and risks.***
5. Exercise: ***Conduct regular training exercises to test and evaluate the emergency response plan and identify areas for improvement.*** This ensures that team members are prepared and can work together effectively in an emergency situation.
By utilizing POETE, organizations can better prepare for and respond to emergencies and disasters, ultimately helping to mitigate the impact on people and property.

If you are not sure if you have properly prepared for a All Hazard event at your facility simple take the highlighted statements and pose them as questions to your Security/Risk Management team. I hope this was helpful!

Jerry G Wilkins, PSP® NREMR® CAHSO® NFPA-3000 Program Specialist
Active Risk Survival, Inc.
Salisbury, Maryland
410-430-1485

J Downs

Apr 24, 2023 4:39 PM
J Downs

Hello,

I was curious if any one else experiences significant delays using AMAG/Symmetry and if they have found any solutions for improving the speed.

Thanks for your time!

J Downs

J Downs
Sr Manager Global Security Programs
Lamb Weston
Eagle ID
United States

View Thread **Like** **Share Discussion** **Flag as Inappropriate**

top previous next

4. Law enforcement recruitment

Reply to Group Online | Reply to Sender Online

Apr 24, 2023 2:04 PM
Dwayne M Gulsby

Police departments are coping with critical staffing shortages and struggling to fill their ranks. Which leaves those serving to work long hours and extra overtime to cover for the shortages.

The main reasons for the recruitment and retention crisis are related to multiple social and political forces, including generational

differences and a negative perception of policing. Just about every police department is looking for the same group of talented motivated individuals.

How do we turn the tide and shake off the negative perception to make the profession attractive to a new generation? Or are we at a new stage that must be adapted to with lower resources, less services and longer wait times?

Dwayne Gulsby CPP
Region President
Securitas Security Services USA, Inc
Frederick MD
United States

View Thread **Like** **Share Discussion** **Flag as Inappropriate**

top previous next

5. Re: Law enforcement recruitment

Reply to Group Online | Reply to Sender Online



Apr 24, 2023 3:28 PM
Kevin Stranahan

Hello Dwayne

It's a great question. At the local level, I can say that some solutions can involve revisiting police-community partnerships and community relations. I attend my local Compstat meetings very other week and the NHPD is trying to return to many of these initiatives, even despite their short staffing. Much of it can also involve salary equity. In 1997, my starting salary with the NYPD was $27,838. More than twenty five years later, that same starting salary is now only around $42,500. Here in CT, some departments also did away with defined pension plans, which resulted in top talent leaving for other agencies.

The discussion has also (of course) impacted healthcare. In speaking with a CEO from Nuvance Health last week, she admitted to me having to resort to recruiting clinical staff from overseas in order to mitigate attrition in healthcare-critical positions.

Kevin J. Stranahan, CFE, CCI, CPP, PCI, PSP
Director of Risk Management & Safety
Fair Haven Community Health Care
New Haven, CT 06513
203-777-7411

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 24 Apr, 2023 14:04
From: Dwayne M Gulsby
Subject: Law enforcement recruitment

Police departments are coping with critical staffing shortages and struggling to fill their ranks. Which leaves those serving to work long hours and extra overtime to cover for the shortages.

The main reasons for the recruitment and retention crisis are related to multiple social and political forces, including generational differences and a negative perception of policing. Just about every police department is looking for the same group of talented motivated individuals.

How do we turn the tide and shake off the negative perception to make the profession attractive to a new generation? Or are we at a new stage that must be adapted to with lower resources, less services and longer wait times?

Dwayne Gulsby CPP
Region President
Securitas Security Services USA, Inc
Frederick MD
United States
---

6. Re: Law enforcement recruitment

Apr 24, 2023 7:02 PM
Brian S Ishikawa

The situation that you wrote about is further negatively impacted by the difficulty that the private sector has faced with hiring and retaining guard staff. This variable makes the dilemma more complex.

Brian Ishikawa CPP
Director of Corporate Security
Bank of Hawaii
Honolulu HI
United States

Original Message:
Sent: 24 Apr, 2023 14:04
From: Dwayne M Gulsby
Subject: Law enforcement recruitment

Police departments are coping with critical staffing shortages and struggling to fill their ranks. Which leaves those serving to work long hours and extra overtime to cover for the shortages.

The main reasons for the recruitment and retention crisis are related to multiple social and political forces, including generational differences and a negative perception of policing. Just about every police department is looking for the same group of talented motivated individuals.

> How do we turn the tide and shake off the negative perception to make the profession attractive to a new generation? Or are we at a new stage that must be adapted to with lower resources, less services and longer wait times?
>
> ---
> Dwayne Gulsby CPP
> Region President
> Securitas Security Services USA, Inc
> Frederick MD
> United States
> ---

top previous next

7. Re: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

Reply to Group Online | Reply to Sender Online



Apr 24, 2023 8:09 AM
Salvatore A D'Agostino

So I put a lot of those cameras in toll booths and having a chain of custody and access control to the video makes a big difference if you are talking about evidence. Also be clear about the fact that the area is under surveillance, I am in the business and big proponent of signs that convey required and useful notice. Camera selection, leasing, lighting will depend, per usual on the scene conditions. And as mentioned by@Michael A Silva these are only a piece of the security system.

Traffic flow, lighting (sensor triggered, even a live display and saying that recording is taking place are some of the other considerations besides the sign. The sign itself should not simply say "area under surveillance", but also provide other useful information about applicable laws and also a point of contact, so that it is understood that there is something/someone responsible behind the camera.

PS, cameras have gotten a lot better wrt performance/price.

Salvatore D'Agostino
CEO
IDmachines
Brookline MA
United States

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 22 Apr, 2023 16:10
From: David Olmstead
Subject: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

A hot topic for many Neighborhood Homeowner Associations (HOAs) is the deterrent value of surveillance cameras at the entrance/exit to the HOA neighborhood. The questions are usually framed in terms of non-operating (i.e., fake) cameras being the most inexpensive but may carry liability issues, real cameras that provide low quality video of little evidentiary value in capturing and convicting a perpetrator, versus something like the more expensive License Plate Cameras (LPCs) that require well planned placement to actually capture the License Plate (sometimes requiring more cameras than originally anticipated and therefore at an increased cost because of performance design requirements).

I have even heard HOA members claim that since there was a break-in, if the HOA does not do something to improve security and there is another break-in the HOA can be sued for failing to act to improve security. I dismissed this as overreach. Even though an HOA is incorporated, it is different than a business that does have an obligation to act because they are inviting people into their establishment. Adding security to a public road is not an obligation of the HOA.

It is over 20 years since I considered this issue, so I am looking for any recent studies or standards.
My previous assessments and current opinion generally come down to the following:
1. Fake cameras are generally a bad idea because they do not actually provide anything of value and carry a liability issue (even if small, it outweighs the nearly nonexistent deterrent value).
2. Back when I previously looked at this issue, the average camera systems gave low quality images, and the recordings (often analog) made things even worse. The evidentiary value might point law enforcement in a direction (e.g., color of vehicle, maybe vehicle make and model, etc.). Unless the surveillance system was well designed, details were hard to observe.
3. Today we have LPCs that can easily capture the license number (sometimes

requiring vehicle information for definitive capture) and a toll bill is sent to the vehicle owner. This indicates a high evidentiary value, but again requires good system design. Its deterrent value will follow a history of effective use by law enforcement. If it is not effective in identifying perpetrators (or at least their vehicles) its deterrent value will be low just as it is with old analog cameras.

I still believe this today, and that the ultimate answer is in the cost/benefit. Do the HOA "members" want the benefit promised at the cost to achieve it.

Thank you all, in advance, for your time at weighing in.

David Olmstead
CPP, FL, United States
---

top previous next

8. Re: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

Reply to Group Online | Reply to Sender Online

Apr 24, 2023 8:10 AM
Felix A Giannini FPE

For all ASIS members, Michael's observations on a better path to more effective security can be best understood, for all security practitioners from entry level to CPP, by spending 3.5 hours garnering the ASIS Enterprise Security Risk Management ESRM certificate. I believe all ASIS members, including CPP's, should use this educational opportunity to allow our membership to communicate more effectively when representing our profession. Overarching inclusive ESRM is our future.

Best, Felix

Felix Giannini FPE

felix@lexcosecurity.com
(203)257-2570

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 22 Apr, 2023 16:10
From: David Olmstead
Subject: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

A hot topic for many Neighborhood Homeowner Associations (HOAs) is the deterrent value of surveillance cameras at the entrance/exit to the HOA neighborhood. The questions are usually framed in terms of non-operating (i.e., fake) cameras being the most inexpensive but may carry liability issues, real cameras that provide low quality video of little evidentiary value in capturing and convicting a perpetrator, versus something like the more expensive License Plate Cameras (LPCs) that require well planned placement to actually capture the License Plate (sometimes requiring more cameras than originally anticipated and therefore at an increased cost because of performance design requirements).

I have even heard HOA members claim that since there was a break-in, if the HOA does not do something to improve security and there is another break-in the HOA can be sued for failing to act to improve security. I dismissed this as overreach. Even though an HOA is incorporated, it is different than a business that does have an obligation to act because they are inviting people into their establishment. Adding security to a public road is not an obligation of the HOA.

It is over 20 years since I considered this issue, so I am looking for any recent studies or standards.
My previous assessments and current opinion generally come down to the following:
1. Fake cameras are generally a bad idea because they do not actually provide anything of value and carry a liability issue (even if small, it outweighs the nearly nonexistent deterrent value).
2. Back when I previously looked at this issue, the average camera systems gave low quality images, and the recordings (often analog) made things even worse. The evidentiary value might point law enforcement in a direction (e.g., color of vehicle, maybe vehicle make and model, etc.). Unless the surveillance system was well designed, details were hard to observe.
3. Today we have LPCs that can easily capture the license number (sometimes requiring vehicle information for definitive capture) and a toll bill is sent to the vehicle owner. This indicates a high evidentiary value, but again requires good system design. Its deterrent value will follow a history of effective use by law enforcement. If it is not effective in identifying perpetrators (or at least their vehicles) its deterrent value will be low just as it is with old analog cameras.

I still believe this today, and that the ultimate answer is in the cost/benefit. Do the HOA "members" want the benefit promised at the cost to achieve it.

Thank you all, in advance, for your time at weighing in.

David Olmstead
CPP, FL, United States
---

top previous next

9. Re: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

Reply to Group Online | Reply to Sender Online

Apr 24, 2023 9:25 AM
Steven J Siegel

Cameras with out response or action are ... well that depends on the reason why the camera is being used... what is it supposed to be doing... why is it there? Proactive camera monitoring and response to incidents are the key. Utilizing a company or SOC that can monitor and respond to a situation seen on a camera IS the reactive means needed to deter future situations. The situation seen on camera IS happening, all that can be done once a situation happens is to respond and take action and make adjustments to deter a similar situation from happening again. A SOC, honestly like ours at St. Moritz Security Services, does that - responds accordingly. The key is the response, not the camera.

Steve Siegel
St. Moritz Security Services
219-900-3382

Steven Siegel
Midwest Vice President & Sales

St. Moritz Security Services
Valparaiso IN
United States

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 23 Apr, 2023 02:30
From: Michael Silva
Subject: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

I am an independent security consultant that has done hundreds of security assessments at multifamily properties. I have written a book and many articles on the subject. It is my opinion that while cameras can be a useful tool in HOA settings, they are not a solution in themselves and should be only one small part of a comprehensive security program.

I feel that cameras have little deterrent effect. I have viewed countless hours of video recordings showing offenders blatantly committing crimes in front of cameras, some even laughing and waving their finger in the well-known manner towards the camera. Even if good quality recordings are obtained, the law enforcement agencies and prosecutors in many jurisdictions don't have the resources to locate, arrest, and prosecute criminals who commit minor property crimes. Most criminals know this and therefore have no reason to be deterred by a camera.

HOAs should review the extent of their security responsibilities with their legal counsel. While the responsibility for the security of individual homes is usually the responsibility of the homeowner, the security of common areas is often the responsibility of the HOA and failure to take adequate steps to protect these areas can result in lawsuits alleging "negligent security".

I feel that HOA's, like any other organization, need to take a comprehensive approach to security. This approach should include operational security measures (policies and procedures, training, security staffing, etc.), physical security (fencing, gates, lighting, landscaping, etc.), and security technology (access control, video surveillance, intrusion detection, etc.) I think that HOAs who put up a few cameras and expect these to solve all of their security problems are likely to be disappointed.

Michael Silva CPP
Principal
Silva Consultants
Covington WA

United States

top previous next

10. Re: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

Reply to Group Online | Reply to Sender Online

Apr 24, 2023 9:29 AM
Jeremiah Main

store.asisonline.org/...

Jeremiah Main PSP
Security Solutions Architect
Granilux Solutions

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 24 Apr, 2023 08:09
From: Felix A Giannini FPE
Subject: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

For all ASIS members, Michael's observations on a better path to more effective security can be best understood, for all security practitioners from entry level to CPP, by spending 3.5 hours garnering the ASIS Enterprise Security Risk Management ESRM certificate. I believe all ASIS members, including CPP's, should use this educational opportunity to allow our membership to communicate more effectively when representing our profession. Overarching inclusive ESRM is our future.

Best, Felix

Felix Giannini FPE
felix@lexcosecurity.com
(203)257-2570

11. Re: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

Reply to Group Online | Reply to Sender Online

Apr 24, 2023 9:37 AM
Jeremiah Main

David,

I spent many years running the security programs at well over a hundred HOA's. During that time I maintained my certification as a manager of community associations (CMCA) through the Community Association Institute. I can tell you that your question regarding liability and case law is being asked and answered in that organization. I can tell you from legal seminars that I sat in (not legal counsel) that they gave many case law examples of HOA's loosing legal battles over the very situation you describe in your question, and that Duty of Care is a real thing for HOA's. If you want to hear for yourself, I recommend connecting with the professionals: www.caionline.org/Advocacy/LegalArena/Pages/...
Hope that helps.

Jeremiah Main PSP
Security Solutions Architect
Granilux Solutions

View Thread Like Share Discussion Flag as Inappropriate

Original Message:

Sent: 22 Apr, 2023 16:10
From: David Olmstead
Subject: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

A hot topic for many Neighborhood Homeowner Associations (HOAs) is the deterrent value of surveillance cameras at the entrance/exit to the HOA neighborhood. The questions are usually framed in terms of non-operating (i.e., fake) cameras being the most inexpensive but may carry liability issues, real cameras that provide low quality video of little evidentiary value in capturing and convicting a perpetrator, versus something like the more expensive License Plate Cameras (LPCs) that require well planned placement to actually capture the License Plate (sometimes requiring more cameras than originally anticipated and therefore at an increased cost because of performance design requirements).

I have even heard HOA members claim that since there was a break-in, if the HOA does not do something to improve security and there is another break-in the HOA can be sued for failing to act to improve security. I dismissed this as overreach. Even though an HOA is incorporated, it is different than a business that does have an obligation to act because they are inviting people into their establishment. Adding security to a public road is not an obligation of the HOA.

It is over 20 years since I considered this issue, so I am looking for any recent studies or standards.
My previous assessments and current opinion generally come down to the following:
1. Fake cameras are generally a bad idea because they do not actually provide anything of value and carry a liability issue (even if small, it outweighs the nearly nonexistent deterrent value).
2. Back when I previously looked at this issue, the average camera systems gave low quality images, and the recordings (often analog) made things even worse. The evidentiary value might point law enforcement in a direction (e.g., color of vehicle, maybe vehicle make and model, etc.). Unless the surveillance system was well designed, details were hard to observe.
3. Today we have LPCs that can easily capture the license number (sometimes requiring vehicle information for definitive capture) and a toll bill is sent to the vehicle owner. This indicates a high evidentiary value, but again requires good system design. Its deterrent value will follow a history of effective use by law enforcement. If it is not effective in identifying perpetrators (or at least their vehicles) its deterrent value will be low just as it is with old analog cameras.

I still believe this today, and that the ultimate answer is in the cost/benefit. Do the HOA "members" want the benefit promised at the cost to achieve it.

Thank you all, in advance, for your time at weighing in.

David Olmstead

CPP, FL, United States
---

top previous next

12. Re: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

Reply to Group Online | Reply to Sender Online

Apr 24, 2023 11:48 AM
Dwayne Cooney

Hi David,

You've brought up some valid points.

While an HOA is responsible for common area maintenance and enforcing community rules, they are generally not liable for criminal activity within the neighborhood. However, it is understandable that an HOA would want to take proactive measures to deter crime. Fake cameras offer little deterrent value and can create liability issues for the HOA.

One of the biggest challenges with implementing a surveillance system in an HOA is providing power and connectivity for retrieving the images. Once those issues are resolved, License Plate Cameras (LPCs) are relatively straightforward to use.

Another consideration is the requirement for front license plates in each state. Some states do not require or enforce front plates, which can affect camera placement and the number of cameras needed.

It's worth noting that A.I. based License Plate Recognition (LPR) is more forgiving than traditional Optical Character Recognition (OCR) based LPR. A.I. based LPR can capture plate images at difficult angles and even in low illumination. Additionally, A.I. LPR can provide searchable data such as plate number, state, vehicle make, body style, color, direction of travel, and more.

There are several A.I. LPR solutions available on the market, including Flock. However, these options can be expensive, with

leasing costing around $2,500 per year and installation and configuration ranging around $350 to $1,100 per camera. For an HOA, this cost can be prohibitive.

A more cost-effective option could be the Rekor Edge series, which allows the HOA to purchase the hardware and subscribe to the cloud-based A.I. service, Rekor Scout. Cellular and non-cellular models, as well as solar and battery kits, are also available.

Alternatively, individual homeowners could explore LPC/LPR options without involving the HOA.

Dwayne Cooney
Physical Security Technology Manager - Americas
Bayer U.S., LLC
Inventor of PlateWatch®

View Thread **Like** **Share Discussion** **Flag as Inappropriate**

Original Message:
Sent: 22 Apr, 2023 16:10
From: David Olmstead
Subject: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

A hot topic for many Neighborhood Homeowner Associations (HOAs) is the deterrent value of surveillance cameras at the entrance/exit to the HOA neighborhood. The questions are usually framed in terms of non-operating (i.e., fake) cameras being the most inexpensive but may carry liability issues, real cameras that provide low quality video of little evidentiary value in capturing and convicting a perpetrator, versus something like the more expensive License Plate Cameras (LPCs) that require well planned placement to actually capture the License Plate (sometimes requiring more cameras than originally anticipated and therefore at an increased cost because of performance design requirements).

I have even heard HOA members claim that since there was a break-in, if the HOA does not do something to improve security and there is another break-in the HOA can be sued for failing to act to improve security. I dismissed this as overreach. Even though an HOA is incorporated, it is different than a business that does have an obligation to act because they are inviting people into their establishment. Adding security to a public road is not an obligation of the HOA.

It is over 20 years since I considered this issue, so I am looking for any recent studies or standards.

My previous assessments and current opinion generally come down to the following:
1. Fake cameras are generally a bad idea because they do not actually provide anything of value and carry a liability issue (even if small, it outweighs the nearly nonexistent deterrent value).
2. Back when I previously looked at this issue, the average camera systems gave low quality images, and the recordings (often analog) made things even worse. The evidentiary value might point law enforcement in a direction (e.g., color of vehicle, maybe vehicle make and model, etc.). Unless the surveillance system was well designed, details were hard to observe.
3. Today we have LPCs that can easily capture the license number (sometimes requiring vehicle information for definitive capture) and a toll bill is sent to the vehicle owner. This indicates a high evidentiary value, but again requires good system design. Its deterrent value will follow a history of effective use by law enforcement. If it is not effective in identifying perpetrators (or at least their vehicles) its deterrent value will be low just as it is with old analog cameras.

I still believe this today, and that the ultimate answer is in the cost/benefit. Do the HOA "members" want the benefit promised at the cost to achieve it.

Thank you all, in advance, for your time at weighing in.

David Olmstead
CPP, FL, United States
---

top previous next

13. Re: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

Reply to Group Online | Reply to Sender Online



Apr 24, 2023 1:21 PM
Jeffry Queen

I agree with Michael. In today's environment, offenders are actively performing in front of cameras. Rather than looking at it from a deterrent perspective, the key question should be on effectiveness of the system in identifying offenders for future apprehension and prosecution. Cameras should simply be one more layer of CPTED.

Jeffry Queen
Head of Corporate Security and Asset Protection
Americano Media
Miami, FL
205-246-0708
jqueen@americanomedia.com

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 22 Apr, 2023 16:10
From: David Olmstead
Subject: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

A hot topic for many Neighborhood Homeowner Associations (HOAs) is the deterrent value of surveillance cameras at the entrance/exit to the HOA neighborhood. The questions are usually framed in terms of non-operating (i.e., fake) cameras being the most inexpensive but may carry liability issues, real cameras that provide low quality video of little evidentiary value in capturing and convicting a perpetrator, versus something like the more expensive License Plate Cameras (LPCs) that require well planned placement to actually capture the License Plate (sometimes requiring more cameras than originally anticipated and therefore at an increased cost because of performance design requirements).

I have even heard HOA members claim that since there was a break-in, if the HOA does not do something to improve security and there is another break-in the HOA can be sued for failing to act to improve security. I dismissed this as overreach. Even though an HOA is incorporated, it is different than a business that does have an obligation to act because they are inviting people into their establishment. Adding security to a public road is not an obligation of the HOA.

It is over 20 years since I considered this issue, so I am looking for any recent studies or standards.
My previous assessments and current opinion generally come down to the following:
1. Fake cameras are generally a bad idea because they do not actually provide anything of value and carry a liability issue (even if small, it outweighs the nearly nonexistent deterrent value).
2. Back when I previously looked at this issue, the average camera systems gave low quality images, and the recordings (often analog) made things even worse. The evidentiary value might point law enforcement in a direction (e.g., color

of vehicle, maybe vehicle make and model, etc.). Unless the surveillance system was well designed, details were hard to observe.
3. Today we have LPCs that can easily capture the license number (sometimes requiring vehicle information for definitive capture) and a toll bill is sent to the vehicle owner. This indicates a high evidentiary value, but again requires good system design. Its deterrent value will follow a history of effective use by law enforcement. If it is not effective in identifying perpetrators (or at least their vehicles) its deterrent value will be low just as it is with old analog cameras.

I still believe this today, and that the ultimate answer is in the cost/benefit. Do the HOA "members" want the benefit promised at the cost to achieve it.

Thank you all, in advance, for your time at weighing in.

David Olmstead
CPP, FL, United States
---

top previous next

14. Re: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

Reply to Group Online | Reply to Sender Online

Jon Polly

Apr 24, 2023 2:16 PM
Jon Polly

Hello,

I am a security technology consultant with a background in policing and citywide surveillance.

Reasons for cameras in HOAs run the gambit, from those that want to "see" everything going on in the neighborhood to those that don't want to be "watched". Common areas such as clubhouses and entryways are typical locations where A) the HOA owns, and B) where crime is possible to happen; i.e. open areas where crowds can gather. This makes a good place to put cameras, but these are not deterrents to criminals as noted by

@Michael A Silva.

HOAs also tend to make decisions based on cost. Many times, the cameras that are installed are of fair quality cameras based solely on price and not quality. The outcome is that even in near-perfect conditions; the cameras are successful to get an image, but not one detailed enough to provide recognition or identification of a person. Recognition here is not a facial biometric, although it could be. Cameras should be placed in the clubhouse, areas where crowds congregate, and to view areas where someone could get hurt, i.e. playgrounds and pools. While there may be a function of deterrence, this is more for an insurance requirement in the event of damage or injury.

License Plate Capture (LPC) as noted has been marginally successful in HOAs. Most LPC cameras are standard 1080p (2MP) cameras running an Optical Character Recognition (OCR) software analytic. Unlike traditional Automated License Plate Recognition (ALPR) cameras which can run upwards of $25K before installation; LPC cameras are significantly cheaper at around $2K - $5K per camera. The reduced cost typically comes with reduced accuracy, using a traditional CCTV imager vs. a black-and-white imager. The LPC works best with slower speeds, in areas of good lighting, and in a closer field of view. Most HOAs have a slow-speed entrance, with plenty of lighting, and a short field of view for the camera to work. These are best-case scenarios and still, most LPCs have an 85% or less accuracy. Here are a couple of articles I have written on the subject of LPC cameras (www.securityinfowatch.com/video-surveillance/...) and (www.securityinfowatch.com/video-surveillance/...)

Property Management companies have little say in what systems they install but may point them to a system integrator. HOAs and Property Management company contracts fluctuate with the changing of the HOA board.

A few notes of specific things to help HOAs avoid problems others have faced.

Policy
To be successful, putting cameras in an HOA requires a well-crafted policy on how long the data will be retained, as well as how the data will be handled. Admirably, many HOAs want to share LPC and camera data with the local police department through a public-private partnership (P3). This is a great idea, however, there must be a defined policy in place on what and how that data is shared, so that those in the HOA who have an expectation of privacy do in fact have that privacy. Not that they are doing illegal actions, but that they give informed consent. The policy should be

reviewed by a legal expert to ensure that the HOA is legal in their actions to share data and that the HOA has a signed Memorandum of Understanding (MOU) with any law enforcement department they are sharing video with; even if a board member is a local law enforcement officer.

Depending on the types of analytics, i.e. facial recognition; a policy with an expressed opt-in by every resident and guest would be required.

Signage
Signage is critical. Signage is a public notice to all entering the property that they are under surveillance and that there is a limited expectation of privacy. It should be affixed to any LPC camera as well as any common areas that are in a camera field of view.

Lighting
Most cameras require a certain amount of ambient light. Law enforcement agencies want only color cameras, even cameras that have IR filters to turn black and white when the lighting is too low don't work because the person and their clothing are not identifiable. Installing cameras without the right amount of lighting is going to waste good money on a system that won't provide the detail desired. Better quality cameras may require less ambient light; the better the lighting, the better the camera image. LPC cameras specifically require a significant amount of ambient light.

Long Term Contracts
Speaking above about LPC cameras, buyer beware. Some of the LPC camera manufacturers (I won't disclose names), sell cameras at a simple yearly price but with required multi-year commitments. These multi-year commitments lock the HOA board in, even if the board changes. Many of these offer cloud services which again points back to data and data retention, locking the HOA board into needing to keep the service because of the data retained. As stated above, LPC cameras can be great tools, but HOAs can become a target of their own want to eliminate crime.

Security isn't just cameras
The term defense in depth still applies here. CPTED strategies, fencing, etc. are all still valid and should be considered as part of the security of the HOA, from multi-tenant buildings to housing neighborhoods.

Jon Polly, PSP, SICC, IC3PM
Chief Solutions Officer

ProTecht Solutions Partners, LLC
(704) 759-6837
Charleston SC
United States
www.linkedin.com/in/JonPolly
www.protechtsolutionspartners.com

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 22 Apr, 2023 16:10
From: David Olmstead
Subject: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

A hot topic for many Neighborhood Homeowner Associations (HOAs) is the deterrent value of surveillance cameras at the entrance/exit to the HOA neighborhood. The questions are usually framed in terms of non-operating (i.e., fake) cameras being the most inexpensive but may carry liability issues, real cameras that provide low quality video of little evidentiary value in capturing and convicting a perpetrator, versus something like the more expensive License Plate Cameras (LPCs) that require well planned placement to actually capture the License Plate (sometimes requiring more cameras than originally anticipated and therefore at an increased cost because of performance design requirements).

I have even heard HOA members claim that since there was a break-in, if the HOA does not do something to improve security and there is another break-in the HOA can be sued for failing to act to improve security. I dismissed this as overreach. Even though an HOA is incorporated, it is different than a business that does have an obligation to act because they are inviting people into their establishment. Adding security to a public road is not an obligation of the HOA.

It is over 20 years since I considered this issue, so I am looking for any recent studies or standards.
My previous assessments and current opinion generally come down to the following:
1. Fake cameras are generally a bad idea because they do not actually provide anything of value and carry a liability issue (even if small, it outweighs the nearly nonexistent deterrent value).
2. Back when I previously looked at this issue, the average camera systems gave low quality images, and the recordings (often analog) made things even worse. The evidentiary value might point law enforcement in a direction (e.g., color of vehicle, maybe vehicle make and model, etc.). Unless the surveillance system was well designed, details were hard to observe.
3. Today we have LPCs that can easily capture the license number (sometimes requiring vehicle information for definitive capture) and a toll bill is sent to the vehicle owner. This indicates a high evidentiary value, but again requires good system

design. Its deterrent value will follow a history of effective use by law enforcement. If it is not effective in identifying perpetrators (or at least their vehicles) its deterrent value will be low just as it is with old analog cameras.

I still believe this today, and that the ultimate answer is in the cost/benefit. Do the HOA "members" want the benefit promised at the cost to achieve it.

Thank you all, in advance, for your time at weighing in.

David Olmstead
CPP, FL, United States
---

top previous next

15. Re: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

Reply to Group Online | Reply to Sender Online



Apr 24, 2023 6:58 PM
Nelson Torres

I agree with your points regarding the limited deterrent effect of cameras and the need for a comprehensive security program in HOA settings.

However, nowadays, cameras can be used as a prevention tool. The advances in video analytics and artificial intelligence allow us to be more proactive than reactive. For instance, smart cameras linked to a video monitoring service can alert authorities when something is out of the ordinary or someone behaves suspiciously. The operator can then issue a warning and call the police immediately. The remote monitoring service can either trigger the warning manually or automate it.

Cameras are now more than just a means of recording video. They can be used in too many applications to prevent criminal activity, get business insights, and more.

Nelson Torres CPP, PSP
Marketing Director
Knight Security Systems
Houston TX
United States

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 23 Apr, 2023 06:27
From: Rafael Espinosa
Subject: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

Interesting topic. Measuring the value of public security initiatives like the ones that are mentioned can only be done through crime and safety perception statistics.

I know of similar initiatives in North America and Europe like community policing, community surveillance patrols, security-related signs and CPTED that have been proven to have a deterrent value for criminal activities.

As for videosurveillance systems in public areas, I believe they are just part of a comprehensive security strategy that must take into account other factors. Sometimes such systems can turn into a problem if personal data treatment practices are not compliant with local regulations, etc.

Rafael Espinosa
Security Engineer

top previous next

16. Re: Electric Vehicle Fire Mitigation?

Reply to Group Online Reply to Sender Online

Apr 24, 2023 10:00 AM
Al Policano

The UL Fire Safety Research Institute (Home | UL's FSRI – Fire Safety Research Institute) has developed quite a few excellent articles/videos on the testing and research they have conducted in association with these types of batteries. The results are pretty staggering to say the least (thermal runaway can create extremely rapid fire growth resulting in much quicker flashover times, extremely difficult to extinguish, toxic fumes being produced, etc.). UL has been working very closely with multiple state fire officials including the FDNY and that partnership has recently resulted in a proposed ban of the sale of all e-bikes/scooters in the City of New York that are not UL-certified. Due to the population density, the amount of e-mobility devices in use, and the vast number of fires experienced already, NYC is taking steps to help ... but this of course is not some ultimate panacea.

Many other factors are at play including user responsibility and product use which will always be a variable. In particular with the impact and vibration that these batteries endure while employed in an e-bike/scooter, battery cells and their associated protection can degrade much more rapidly than the manufacturers have seemed to anticipate.

This topic needs to be treated with a much greater sense of urgency by federal, state, and local municipalities to address the current and future dangers associated with Lithium-Ion batteries, especially considering that these events have the potential to increase exponentially as more and more EV's and e-mobility devices continue to gain adoption with the public.

Al Policano, PSP
Secretary - ASIS School Safety & Security Committee
Principal Engineer - Fire and Security Systems
UL Solutions
Melville, NY

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 20 Apr, 2023 16:30
From: James A Cosseboom
Subject: Electric Vehicle Fire Mitigation?

There have been a growing number of media reports about the issues that fire departments are having with electric vehicle fires that burn much hotter and longer. An interesting article from CNBC is pasted below. Where these are growing in popularity, the number of fires will likely grow.

Has anyone changed your facility response to a fire in one of these vehicles at one of your facilities, especially indoor parking facilities?

www.cnbc.com/2023/04/20/...

James Cosseboom, LPC
Director, Asset Protection
Retail Business Services LLC an Ahold Delhaize USA company
Boston MA
(508) 977-5304
---

top previous next

17. Re: Electric Vehicle Fire Mitigation?

Reply to Group Online | Reply to Sender Online

Apr 24, 2023 1:37 PM
Timothy Diehl

As a member of both NFPA and ICC, I know there are multiple conversations being held concerning EV's, ESS, and Lithium Ion batteries. Not only relating to FD and Security response but also manufacturing, storage, and recycling. Yes the Codes don't fully address all the issues we are facing but the groups are working hard to provide information in a timely fashion. Listed below are links for current resource material available.

Research background:

fsri.org/research/...

fsri.org/research/impact-batteries-fire-dynamics

Battery Resources

IAFC Recommended Fire Department Response to Energy Storage Systems - Part 1

www.iafc.org/docs/default-source/1fire-prev/...

IAEI/ICC Energy Storage Systems Based on the IBC, IFC, IRC, and NEC

sustainableenergyaction.org/resources/icc-ess-guide

shop.iccsafe.org/...

There is a separate guide relating to Solar projects which groups have created (IAEI/ICC/NFPA)

IAEI/ICC/NFPA 2021 International Solar Energy Provisions (and commentary as a separate document)

www.iccsafe.org/about/periodicals-and-newsroom/...

shop.iccsafe.org/...

shop.iccsafe.org/...

Hopefully you will find this information of value.

Timothy Diehl APP
Building Security Manager
Howard County Government
Columbia MD
United States
tdiehl@howardcountymd.gov

View Thread **Like** **Share Discussion** **Flag as Inappropriate**

Original Message:
Sent: 20 Apr, 2023 16:30
From: James A Cosseboom
Subject: Electric Vehicle Fire Mitigation?

There have been a growing number of media reports about the issues that fire departments are having with electric vehicle fires that burn much hotter and longer. An interesting article from CNBC is pasted below. Where these are growing in popularity, the number of fires will likely grow.

Has anyone changed your facility response to a fire in one of these vehicles at one of your facilities, especially indoor parking facilities?

www.cnbc.com/2023/04/20/...

James Cosseboom, LPC
Director, Asset Protection
Retail Business Services LLC an Ahold Delhaize USA company
Boston MA
(508) 977-5304
---

top previous next

18. Re: LED Lighting and CCT

Reply to Group Online | Reply to Sender Online

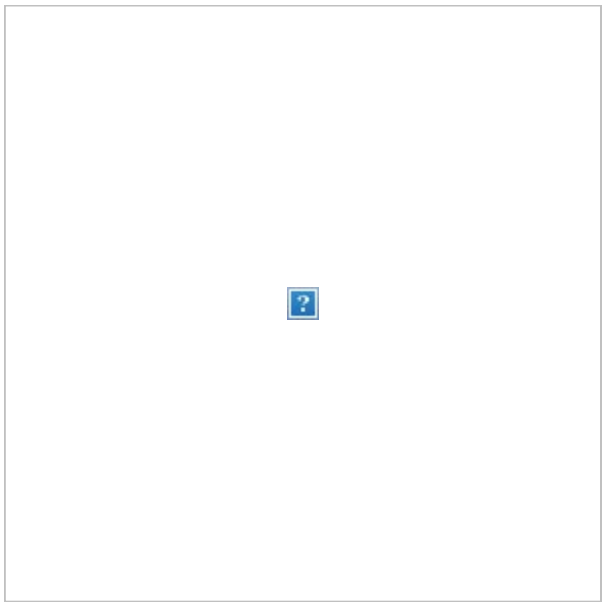
Apr 24, 2023 10:07 AM
Matthew Beausoleil

Sami,

My field of expertise is Perimeter Fence Lighting and integration with security cameras, and motion sensors. Unsure if you are using our product currently, but I would be happy to help you if you want to reach out. mattb@cast-lighting.com

You can see our products in this video also
youtu.be/U024hiuIpiY

Short answer to your question regarding Color Temperature:



Security Lighting should be a balanced white light, 4400K - 4600K we found to be the optimal color temperature for nighttime camera color imaging and human eye facial recognition, 3000K is more of an architectural temperature for landscape lighting, and 5700K can make some colors appear bluer than they actually are, may mis represent colors under a camera.

The other factors that must be considered are things like "Uplight" this can be found in a BUG report, as lights with uplight that are below a camera can cause washout. And light distribution is also incredibly important, as often light is concentrated too much in a single area, and that makes calibration to a camera very difficult, causing washout. 4:1 is the gold standard as it follows the natural dissipation of light and prevents washout, 6:1 can cause washout problems.

I would love to talk to you about your project, we have worked with a few sites in Saudi Arabia.

Our products mount directly on the fence, with a 4:1 min max ratio for camera integration perfection, additionally for 240Watts you can install 25 of our Low power luminaires covering 150 Meters of fenceline, or 10 of our high powered luminaires which cover about 90 Meters. Cameras can achieve color imaging often at under 1 lux, while the NATO spec for fence lighting for Human Security is 5

Lux at 10 Meters, and in our testing, 2.5 lux is bright enough to read a news paper. All of our security luminaires are between 4400-4600K

We wrote the book on perimeter security lighting if you want a free ebook download check out the link below
cast-lighting.com/perimeter-ebooks/...

Thank you,

Matthew Beausoleil
Security Lighting Designer
CAST Lighting
Southern Pines NC
United States

View Thread **Like** **Share Discussion** **Flag as Inappropriate**

Original Message:
Sent: 20 Apr, 2023 07:08
From: Sami Mohammad Daoud Adwan
Subject: LED Lighting and CCT

Hello Everyone
We are installing Led Lighting along the fence that protecting industrial facility, the Led is coming with different CCT such as (3000K, 4000K and 5700K). which one is the suitable CCT to choose for security patrolling as well as for security operators whom monitoring the facility perimeter?

Sami Mohammad Daoud Adwan PSP
Senior Project Engineer
NUDHUM
Riyadh
Saudi Arabia
---

19. Re: Training and Development in Video Surveillance Systems

Reply to Group Online | Reply to Sender Online

Apr 24, 2023 11:14 AM
Dwayne Cooney

NICET
www.nicet.org/certification-programs/...

IPVM:
ipvm.com/training

ESA
courses.esaweb.org/shop

Axis
www.axis.com/learning/academy/learning-portal

Dwayne Cooney
Physical Security Technology Manager - Americas
Bayer U.S., LLC
Inventor of PlateWatch®

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 19 Apr, 2023 08:15
From: Richard P Laib
Subject: Training and Development in Video Surveillance Systems

Hello-I am looking to develop in my knowledge of video surveillance systems installation. Would anyone be able to recommend a beginner's course or

conference?

Thank you!

Rick Laib
Joliet IL
United States
---

top previous

20. Re: Photos on access cards, good or bad for security?

Reply to Group Online



Apr 24, 2023 4:47 PM
Anonymous Member

This message was posted by a user wishing to remain anonymous

I feel it is a best practice, along with color coding. For example, one color for full-time employees, one for contractors, and another for visitors.

Although, there was a time when one of our managers tested the use of photos by creating a badge for himself with a completely different photo. He wore the badge for a week and was not questioned once.

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 14 Apr, 2023 14:50
From: Anonymous Member

Subject: Photos on access cards, good or bad for security?

This message was posted by a user wishing to remain anonymous

I'm struggling to understand the merits of putting employee photos on access cards for the purpose of security if it's not expected to be checked. If it's lost in the street, I can find it and target you. If it's forgotten at home, there's nothing for the guard to check. If it's in the employee's pocket all day, no one sees it. If it's around the employee's neck and no one's checking it, it's doesn't make a difference.

Any help here to agree or disagree would be great. I'm debating the point of introducing mobile phone as a card (has a digital photo, hard to loose, low environmental waste, works at every office and for traveling employees, easy to deactivate, etc.) instead of spending the time and dollars on photos on cards at every location.

You are subscribed to "Open Forum" as paul.upton@pol.state.ma.us. To change your subscriptions, go to My Subscriptions.

From: ASIS International
To: Upton, Paul (POL)
Subject: Open Forum Digest for Monday March 6, 2023
Date: Tuesday, March 7, 2023 1:48:05 AM

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

Open Forum

Post New Message

Mar 6, 2023

Discussions

started yesterday, Michael R Sparks (3 replies)

Stand alone Lost & Found program

1. Good Morning Michael, I run security for 3... Anthony Norcia
2. Michael, Take a look the Owens Group, one... Ronald E Grimes
3. Hey Michael - when I was with Four Seasons, we... Robert R Currie

started 3 days ago, Charles Chang (8 replies)

Vehicle license plate readers

4. What is the location? What are the business... Dwayne Cooney
5. Hello Charles, I previously posted in your drone... Igor Keel

started 5 days ago, Anonymous Member (9 replies)

Email for Alarm Notifications

6. Hello Anonymous poster, I believe what you're... Igor Keel

started 5 days ago, Eric Donaldson (4 replies)

Google Street View

7. This message was posted by a user wishing to... Anonymous Member

started one month ago, Eric Davoine (51 replies)

ChatGPT and Security

8. I will definitely look into that. And of course... David Evans
9. Thanks for the thoughts Eric & others, it's an... Shayne P Bates

top next

1. Re: Stand alone Lost & Found program

Reply to Group Online | Reply to Sender Online

Mar 6, 2023 7:05 AM
Anthony Norcia

Good Morning Michael,

I run security for 3 resorts in Myrtle Beach, South Carolina, about 900 rooms combined. We use Chargerback.com as our standalone L&F platform. They offer shipping through USPS, UPS and Fed Ex. The website is easy to manage. Their customer service and tech support are responsive. The one and only downside is they're a bit pricy. Another option is Ileftmystuff.com. Their prices are more reasonable and offer several different shipping options. Feel free to reach out to me to discuss 843-274-8846

Anthony Norcia CPP, PCI, PSP
Loss Prevention Director
Hilton Grand Vacations
Myrtle Beach SC
United States

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 05 Mar, 2023 18:59
From: Michael R Sparks
Subject: Stand alone Lost & Found program

I'm looking for recommendations for a stand alone Lost & Found program suitable for use at a 375 room hotel with large event spaces. Formally, my department used MS Shift which had a good Lost & Found module, but had to give it up when the company decided to go to a single, standard security management program across all of its properties. The new program is generally pretty good, but it mixes Lost &

> Found reports with every other report generated. This has made searching for specific items difficult and our process less efficient for returning found property to guests.
>
> ---
> Michael Sparks CPP, PSP
> Silver Spring MD
> (240)887-7698
> ---

top previous next

2. Re: Stand alone Lost & Found program

Reply to Group Online | Reply to Sender Online

Mar 6, 2023 8:34 AM | view attached

Ronald E Grimes

Michael,

Take a look the Owens Group, one of the largest, most organized lost & found services I found and will be using. The service is a win-win for the guest and for you as the client.

The Owens Group

Ron Grimes
Director of Safety & Security
Ryman Hospitality Properties
Nashville, TN
615-316-6318
www.rymanhp.com
rgrimes@rymanhp.com

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 05 Mar, 2023 18:59
From: Michael Sparks
Subject: Stand alone Lost & Found program

I'm looking for recommendations for a stand alone Lost & Found program suitable for use at a 375 room hotel with large event spaces. Formally, my department used MS Shift which had a good Lost & Found module, but had to give it up when the company decided to go to a single, standard security management program across all of its properties. The new program is generally pretty good, but it mixes Lost & Found reports with every other report generated. This has made searching for specific items difficult and our process less efficient for returning found property to guests.

Michael Sparks CPP, PSP
Silver Spring MD
(240)887-7698
---

top previous next

3. Re: Stand alone Lost & Found program

Reply to Group Online | Reply to Sender Online

Mar 6, 2023 9:20 AM
Robert R Currie

Hey Michael - when I was with Four Seasons, we were looking at ChargerBack across the brand as some locations had implemented it with success.

Cheers

/rob

Robert Currie
Owner & founder
RCAS
Ottawa ON
Canada
16139794346

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 05 Mar, 2023 18:59
From: Michael R Sparks
Subject: Stand alone Lost & Found program

I'm looking for recommendations for a stand alone Lost & Found program suitable for use at a 375 room hotel with large event spaces. Formally, my department used MS Shift which had a good Lost & Found module, but had to give it up when the company decided to go to a single, standard security management program across all of its properties. The new program is generally pretty good, but it mixes Lost & Found reports with every other report generated. This has made searching for specific items difficult and our process less efficient for returning found property to guests.

Michael Sparks CPP, PSP
Silver Spring MD
(240)887-7698
---

top previous next

4. Re: Vehicle license plate readers

Reply to Group Online Reply to Sender Online

Mar 6, 2023 9:37 AM
Dwayne Cooney

What is the location? What are the business requirements?

Dwayne Cooney
Physical Security Specialist, Patent Pending Inventor
LinkedIn: www.linkedin.com/in/dwaynecooney

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 03 Mar, 2023 10:14
From: Charles Chang
Subject: Vehicle license plate readers

Hi all,

Assessing vehicle plate reader capability for potential implementation on a large campus. Would appreciate your experience with the system and any pros-cons you've experienced. Of course, any recommendation of solid products are also welcomed. Thanks in advance. Charles

---
Charles Chang
Senior Director, Global Physical Security
Lam Research
Pyeongtaek
---

top previous next
5. Re: Vehicle license plate readers
Reply to Group Reply to Sender

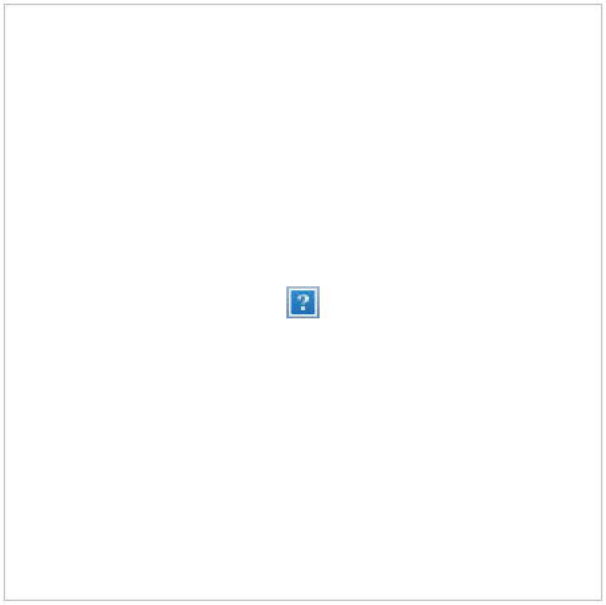
Online | Online

Igor Keel

Mar 6, 2023 12:00 PM | view attached

Igor Keel

Hello Charles, I previously posted in your drone surveillance thread. Similarly, my recommendation is to evaluate cloud-based technology to potentially satisfy your ALPR requirements. In your situation, if an internet connection can be provided to existing cameras, their encrypted video feed can be extended directly to the cloud servers (public or private, your preference), for ALPR video post-processing with the option only to view the feed of recognized results as far back as you need, but also set customized alerts for preset plates, and perform textual search for previous results, with easy video event sharing abilities.



Per your request, Pros would be the ease of deployment to existing video security (no need to buy additional hardware or replace cameras), low monthly subscription fee to layer cloud-based intelligence, flexible video streaming requirements (the pictured camera in the example is an inexpensive 1 MP camera), extend to unlimited simultaneous viewing and administration stakeholders, and the only Con I can think of is that internet connectivity is required, though at least you can avoid the networking hassles of port forwarding or opening any firewall ports.

---

www.3deye.me (Professional Cloud Video Surveillance and

Analytics Platform)
ASIS member since 2020

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 03 Mar, 2023 10:14
From: Charles Chang
Subject: Vehicle license plate readers

Hi all,

Assessing vehicle plate reader capability for potential implementation on a large campus. Would appreciate your experience with the system and any pros-cons you've experienced. Of course, any recommendation of solid products are also welcomed. Thanks in advance. Charles

---
Charles Chang
Senior Director, Global Physical Security
Lam Research
Pyeongtaek
---

top previous next

6. Re: Email for Alarm Notifications

Reply to Group Online | Reply to Sender Online

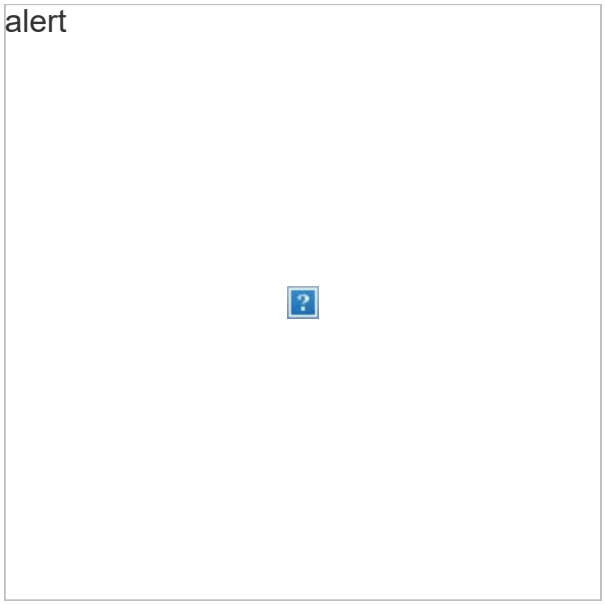
Igor Keel

Mar 6, 2023 11:48 AM
Igor Keel

Hello Anonymous poster, I believe what you're looking for are *webhooks*; alerts can be configured to trigger different hardware if your program allows settings up webhooks. Triggers can lead to automatic sequences programmed in popular solutions

such as Zapier and IFTTT. These services can make calls, send SMS, among many options, or trigger different hardware (often via a RasPi). It can be setup as simply or complex as you need it. For example, I have a sequence setup where when the predefined video intrusion is detected in my cloud cameras it triggers this smart outlet to turn on, which not only triggers on-site deterrence but alerts me by turning on certain lights. There are many similar *smart* devices to that plug which could also be useful. But if you simply want to be notified via SMS or an automated phone call, that could also be set up with a service like IFTTT, though be prepared to pay a service fee. I previously had the service call my phone in case my inbox received a predefined email and an automated voice read out the message which was emailed. Below is an example of the type of email which triggered the phone call. Latency must be prioritized if you want to receive the alerts in a timely manner, but in my case latency was sufficient as the platform delivered object-recognized alerts in sub-second latency and the call was made shortly thereafter.

alert



---
www.3deye.me (Professional Cloud Video Surveillance and Analytics Platform)
ASIS member since 2020

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 01 Mar, 2023 14:45

From: Anonymous Member
Subject: Email for Alarm Notifications

This message was posted by a user wishing to remain anonymous

Alarm Notification by Email: Is it becoming more common for intrusion alarm activations to only be communicated by email? This may be better than no alarm at all; but it seems inefficient, and possibly ineffective (I.e. by the time I see the email on my phone, the burglary or intrusion is already well underway). Any comments or advice is appreciated.

top previous next

7. Re: Google Street View

Reply to Group Online

Mar 6, 2023 3:45 PM
Anonymous Member

This message was posted by a user wishing to remain anonymous

Adding to the information on blurring for Google Maps. I read that other countries may or may not show the same blurring so you may wish to ask questions of Google Maps regarding that issue.

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 02 Mar, 2023 09:30
From: Dhario DeSousa
Subject: Google Street View

Hi Eric,

Echoing what Kristof posted: relatively easy to blur the facade of a building from Google Maps as long as you have the right to do so (e.g., you own the building). Redactions are permanent. You should also pursue other mapping services such as

Bing Maps.

Best,

Dhario DeSousa
Manager, Intelligence
Direct: (917) 635-8690
O: (212) 362-5700 | (646) 356-2313
www.insiteriskmanagement.com

Dhario DeSousa
New York NY
United States

top previous next

8. Re: ChatGPT and Security

Reply to Group Online | Reply to Sender Online

Mar 6, 2023 5:07 AM
David Evans

I will definitely look into that. And of course as mentioned before. The example I gave was just for fun and we know it's just a mimic for now. But once the platform and the way you can input data is refined then the possibilities become quite staggering. We have software now that can look for insider threats and so on and if they'll continue to be effective once everyone has access to something like this is yet to be seen but it definitely feels like we're in the beginning of the next revolution for sure and I'm excited to see what comes next.

David Evans
Senior Key Account Manager
Nedap Security Management

Haaksbergen
Netherlands

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 05 Mar, 2023 13:24
From: David Spector
Subject: ChatGPT and Security

For a VERY interesting discussion of this topic, the Crisis Management and Business Continuity (CMBC) Community just recorded a video podcast on CHATGPT and AI, which will be released on March 23, on the CMBC Community Connects page. Our guests, Tony Ridley and Peter Warmka, will speak with host Andrew Peden, CMBC Chair Rob Currie and Communications Expert Ernest DelBuono regarding security concerns, social engineering challenges, how to best use CHATGPT, and other important issues.

Watch for the posting in a few weeks!

David Spector CPP
Sr Security Administrator
MIT Lincoln Laboratory
Acton MA
United States

top previous

9. Re: ChatGPT and Security

Reply to Group Online | Reply to Sender Online



Mar 6, 2023 10:24 AM | view attached

Shayne P Bates

Thanks for the thoughts Eric & others, it's an interesting topic to

me. I've been reading about ChatGPT for some time.

So far I've resisted jumping in to work with it, instead reading what others who are doing so have to say with their tests to leverage my understanding through their learning experiences and thoughts.

This approach is bearing fruit for me to understand the broader use cases and applications for the tool so far. What's even more interesting are the types of emergent AI tools and the various categories that they fit as perceived by the contributors.

In the case of ChatGPT, the comments also included whether it is the paid version or the freebie as both have different capabilities.

Along the way I've discovered an interesting FaceBook group entitled "ChatGPT Community". It has 224,000 members and growing. For those who want to join and see that in your feed, much of it you will want to scroll past, but several of these each day are an interesting read for education.

There are 3 images attached with this post. The first is a description about the group, while the second and third are images posted by others, which I found helpful. Remember, they are just opinions, not facts, but useful to see what others are saying.

All the best

Shayne

Shayne P. Bates, CPP
North America: Texas +1 (512) 645-7420
Asia Pacific + 64 (9) 889-4253

Web http://www.stratum-knowledge.com
Twitter https://twitter.com/shaynebates
LinkedIn www.linkedin.com/in/shaynebates

Stratum Knowledge LLC. DBA Shayne Bates
PO Box 261, Paige, TX 78659

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 17 Jan, 2023 03:17
From: Eric Davoine
Subject: ChatGPT and Security

Hello all,
I'm a bit surprised as I didn't notice any post on this topic so far (I may have missed one!). So... let's start!

I guess (hope!) you all heard about ChatGPT and it's an incredible AI based chatbot. I'm wondering who has already used/tried it and for which purpose.
So let's start. I asked several questions to the tool and I'm pleased to share its answers. You will see, regarding the Travel Security advices to Nigeria, the Building access control process or a Workplace violence program in Hospitals, that the outcomes are great! and it took an average of 3 to 8 seconds to produce them!
Of course, everybody can (and will, for sure !) criticize the lack of detail and precision. But bear in mind that the purpose of such a tool **is not** to give you an answer that you already know!

So, of course, there are some obvious caveats to take in consideration:
- time frame: the tool does not encompass 2022 data. So do not ask questions requiring such updates
- it's easier to work with threads as the tool keep the context for the following answers (if you plan to dig in a topic)
- and... a tool is a tool and should deserve a purpose... with a level of control!

I really thinks that the outputs incredible at this stage and I'm looking forward its results in 3 years ahead!

Any opinion? advice? Use case?

Best

Eric Davoine CPP
Group Head of Physical Security and Safety
Axa
eric.davoine@axa.com

You are subscribed to "Open Forum" as paul.upton@pol.state.ma.us. To change your subscriptions, go to My Subscriptions.

From: ASIS International
To: Upton, Paul (POL)
Subject: Open Forum Digest for Saturday March 4, 2023
Date: Sunday, March 5, 2023 12:58:17 AM

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

Open Forum

Post New Message

Mar 4, 2023

Discussions

started yesterday, Charles Chang (3 replies)

Vehicle license plate readers

1. Hi Charles, There are several options when... Rafael Espinosa
2. What are you trying to accomplish or do you just... Salvatore A D'Agostino
3. Charles, I have used the Digital Watchdog... Felix A Giannini FPE

started 3 days ago, Anonymous Member (8 replies)

Email for Alarm Notifications

4. These days, alarm notification (to the end user... Felix A Giannini FPE

started one month ago, Eric Davoine (48 replies)

ChatGPT and Security

5. All, This is a good discussion and I... Reginald P Parker

top next

1. Re: Vehicle license plate readers

Reply to Group Online | Reply to Sender Online

Mar 4, 2023 7:51 AM



Rafael Espinosa

Hi Charles,

There are several options when looking for an ALPR (automatic license plate reading) solution. The first and most obvious one is installing a specific number of videosurveillance cameras with ALPR software included. This solution works when you want only specific cameras to use ALPR without making your whole videosurveillance system have this capacity.

The second option is integrating an ALPR engine to your videosurveillance system as an “add-on”. This engine will identify license plate alphanumeric characters based on predefined algorithms that may vary from country to country (as license plates vary from country to country too). This feature may be used for all or part of your videosurveillance system depending on your needs.

As to specific solutions for ALPR, I believe that Genetec Autovu offers a good ALPR solution and advanced integration with other systems such as access control and intrusion detection, cartography, etc. However, the choice for the best solution shall depend on the scope of your project and the specific needs your organization may have.

A good systems integrator may be better suited to understand these needs and explain all the upsides and downsides of each solution.

Hope this is useful!

Rafael Espinosa
Security Engineer

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 03 Mar, 2023 10:14
From: Charles Chang
Subject: Vehicle license plate readers

Hi all,

Assessing vehicle plate reader capability for potential implementation on a large campus. Would appreciate your experience with the system and any pros-cons you've experienced. Of course, any recommendation of solid products are also welcomed. Thanks in advance. Charles

---
Charles Chang
Senior Director, Global Physical Security
Lam Research
Pyeongtaek
---

top previous next

2. Re: Vehicle license plate readers

Reply to Group Online | Reply to Sender Online

Mar 4, 2023 8:17 AM
Salvatore A D'Agostino

What are you trying to accomplish or do you just want to know about current capabilities? Is there an installed base? Where are you doing this ((US?). Have a fair amount of experience here..

Salvatore D'Agostino
CEO
IDmachines
Brookline MA
United States

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 03 Mar, 2023 10:14
From: Charles Chang
Subject: Vehicle license plate readers

Hi all,

Assessing vehicle plate reader capability for potential implementation on a large campus. Would appreciate your experience with the system and any pros-cons you've experienced. Of course, any recommendation of solid products are also welcomed. Thanks in advance. Charles

---
Charles Chang
Senior Director, Global Physical Security
Lam Research
Pyeongtaek
---

top previous next

3. Re: Vehicle license plate readers

Reply to Group Online | Reply to Sender Online

Mar 4, 2023 2:42 PM
Felix A Giannini FPE

Charles,

I have used the Digital Watchdog LPR camera successfully. There are several important considerations including frame rate and camera angle. This is a link to the Digital Watchdog LPR Guide to LPR applications which applies to all brands.

I recommend using non exclusively distributed products so that as the end user you remain in control of the service of the product,

should you decided to change your vendor.

All camera manufacturing companies should be vetted for international watch lists, as some IP cameras and recorders are banned due to "back door" remote access.

I also recommend that all physical security systems be done in concert with a comprehensive ESRM program.

Best wishes,

Felix

Felix Giannini FPE
felix@lexcosecurity.com

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 03 Mar, 2023 10:14
From: Charles Chang
Subject: Vehicle license plate readers

Hi all,

Assessing vehicle plate reader capability for potential implementation on a large campus. Would appreciate your experience with the system and any pros-cons you've experienced. Of course, any recommendation of solid products are also welcomed. Thanks in advance. Charles

---
Charles Chang
Senior Director, Global Physical Security
Lam Research
Pyeongtaek
---

4. Re: Email for Alarm Notifications

Reply to Group Online | Reply to Sender Online



Mar 4, 2023 2:56 PM
Felix A Giannini FPE

These days, alarm notification (to the end user's internal responders) has many options including **phone call, text, email,** in any combination - and by each listed individual **and by SCADA**. Emergency responders are typically dispatched by a recorded phone call made by a qualified central station operator.

Personal Tip: Of critical importance is the "Zone Descriptor" for the individual alarm initiating point. This is often not given the thought it deserves. I believe carful choice *maximizing the allowable description characters* improves response and recovery! I call it "Concierge Monitoring" when zone descriptors go through a review process in an ESRM effort to improve system operability, response, (especially when the alarm if of a life safety concern) and recovery.

Happy to provide more information,

Felix

Felix Giannini FPE
felix@lexcosecurity.com

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 01 Mar, 2023 14:45
From: Anonymous Member
Subject: Email for Alarm Notifications

This message was posted by a user wishing to remain anonymous

> Alarm Notification by Email: Is it becoming more common for intrusion alarm activations to only be communicated by email? This may be better than no alarm at all; but it seems inefficient, and possibly ineffective (I.e. by the time I see the email on my phone, the burglary or intrusion is already well underway). Any comments or advice is appreciated.

top previous

5. Re: ChatGPT and Security

Reply to Group Online Reply to Sender Online



Mar 4, 2023 2:04 AM
Reginald P Parker

All,

This is a good discussion and I believe a protocol or Body of Knowledge (BoK) will be developed within our security field that will necessarily address some of the concerns you have already raised. I fear improper use by "unguided' security practitioners and HR professionals could open the door to liability suits depending on what action is taken by management.

As a professor, I am already seeing papers that I strongly suspect are not the students original work. Faculty have tools to check validity of content and plagiarism but ChatGPT (and others) opens a new concern. I am not certain yet how to challenge some of these students who I know did not write these papers. One of my mitigations last semester was to require all students always come to class with one of the "old school" blue, lined test booklets. I would give a writing quiz to be completed in class and collect the booklets. The embedded test here was to see how they write on their own so that I had a comparison. It is a lot of extra work and with foreign students whose native language is not English, it is even more difficult.

I thnk we hae a lot to consider on this topic and perhaps, am ASIS committee need to be formed and get everne ahead of the curve on this.

Cheers,

Reg

Reginald P. Parker CPP PMP
Professor of Corporate Security
College of Business, Security and Intelligence
Embry-Riddle Aeronautical University
Prescott, AZ

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 03 Mar, 2023 07:37
From: David Evans
Subject: ChatGPT and Security

Ive put ChatGPT through few scenarios now and one that i was interested in that will need some further investigation is using it to identify anomalies in transaction data. If we look at a typical insider threat metric such as 'irregular timings' it becomes clear that although its good, ChatGPT is not perfect.

Below are my prompts and the results. I generated hypothetical data.

David Evans: Below are the check-in and check-out times for and employee called John. Can you find any obvious anomalies?

8:50

17:15

8:02

17:00

8:00

16:50

9:15

17:16

8:14

22:10

8:03

17:50

8:01

17:10

8:15

17:00

7:50

17:01

8:50

17:02

8:02

17:06

8:14

17:20

8:14

23:01

8:14

17:00

ChatGPT:

Without additional context or information, it is difficult to determine any specific anomalies in the data. However, there are a few observations that can be made:

1. The check-in and check-out times generally follow a consistent pattern, with most of the times falling within a similar range.
2. The check-out time for entry 10 (22:10) is significantly later than the other check-out times. This could be a legitimate anomaly or a mistake in the data.
3. There are a few instances where the check-in and check-out times are only a few minutes apart (e.g. entry 5 and 6). While this could be legitimate if the

> employee was only at work for a short period, it is worth investigating further to ensure that the data is accurate.
>
> Overall, it may be helpful to review the data with the employee or their supervisor to clarify any discrepancies and ensure that the data is accurate. Additional context or information, such as the employee's work schedule or job responsibilities, could also be helpful in identifying any anomalies.
>
> **David Evans:** What were the times for entry 5 and 6?
>
> **ChatGPT:**
>
> Entry 5 was a check-in time of 8:00 and entry 6 was a check-out time of 16:50. This suggests that the employee was only at work for a period of 8 hours and 50 minutes, which could be legitimate depending on their work schedule or job responsibilities. However, it is worth investigating further to ensure that the data is accurate and that there are no discrepancies or anomalies.
>
> So you can see that although it picked up the general idea of what we were looking for it did make a few errors. But its a very interesting start
>
> ---
> David Evans
> Senior Key Account Manager
> Nedap Security Management
> Haaksbergen
> Netherlands

You are subscribed to "Open Forum" as paul.upton@pol.state.ma.us. To change your subscriptions, go to My Subscriptions.

From: ASIS International
To: Upton, Paul (POL)
Subject: Open Forum Digest for Tuesday April 25, 2023
Date: Wednesday, April 26, 2023 1:31:47 AM

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

Open Forum

Post New Message

Apr 25, 2023

Discussions

started yesterday, Gerald G Wilkins (4 replies)

Active Shooter Preparedness

1. Hi Gerald, A great framework. Thanks! ... Alan Cranfill
2. Thank you for taking time to read the POETE... Gerald G Wilkins
3. Thank you for taking time to read the summary I... Gerald G Wilkins

started yesterday, J Downs (2 replies)

AMAG/Symmetry Latency + Solutions

4. From time to time we experience lags. We are... Michael Korn
5. Depending on the size of your system, it could... Matthew J Underwood

started yesterday, Dwayne M Gulsby (5 replies)

Law enforcement recruitment

6. Thanks for the response Kevin and I agree there... Dwayne M Gulsby
7. Good morning, Dwayne The 21st century... Oscar Odom
8. Great points Dr. Odom especially with the 4 day... Dwayne M Gulsby

started 3 days ago, David Olmstead (16 replies)

Deterrent value of Cameras at the entrance/exit of a Neighborhood.

9. Hey David, if I may chime in here First and... Charles Jasper
10. There are current studies that show cameras are... Anthony Beattie
11. There is likely little to no deterrent value of... K. Campbell
12. Thanks for the message about Signage and Notice,... Salvatore A D'Agostino

top next

1. Re: Active Shooter Preparedness

Reply to Group Online | Reply to Sender Online



Apr 25, 2023 9:15 AM
Alan Cranfill

Hi Gerald,

A great framework.

Thanks!

Alan Cranfill
Director - Health, Safety and Security
Hines Interests LP
Houston TX
United States

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 24 Apr, 2023 19:35
From: Gerald G Wilkins
Subject: Active Shooter Preparedness

One of the questions I hear most often is, "how do I prepare my organization to respond to an All Hazard event:. I believe researching best practice is always a good place to start. FEMA classifies Active Shooter events as ALL Hazard events. So, I summarized the FEMA POETE framework as a potential good place to start.

POETE (Planning, Organization, Equipment, Training, and Exercise) is a framework used in emergency management and disaster response to ensure effective preparedness and response activities. Here's how you can use POETE:

1. Planning: Develop a comprehensive emergency response plan that outlines the roles and responsibilities of all parties involved in the response effort. ***Identify potential hazards and risks, develop a communications plan, and establish procedures for resource allocation and coordination.***
2. Organization: ***Establish an organizational structure for your emergency response team, including a clear chain of command and designated roles and responsibilities for each member.*** This ensures that everyone knows their role and what they are responsible for during an emergency.
3. Equipment: ***Make sure that all necessary equipment and resources are available and ready for use.*** This includes communication devices, personal protective equipment, medical supplies, and vehicles, among others. Regular maintenance and testing of equipment should also be done to ensure that they are in good working condition.
4. Training: Ensure that all team members have the appropriate training and knowledge required for their roles. ***This includes training on emergency response procedures, the use of equipment, communication protocols, and the identification of potential hazards and risks.***
5. Exercise: ***Conduct regular training exercises to test and evaluate the emergency response plan and identify areas for improvement.*** This ensures that team members are prepared and can work together effectively in an emergency situation.

By utilizing POETE, organizations can better prepare for and respond to emergencies and disasters, ultimately helping to mitigate the impact on people and property.

If you are not sure if you have properly prepared for a All Hazard event at your facility simple take the highlighted statements and pose them as questions to your Security/Risk Management team. I hope this was helpful!

Jerry G Wilkins, PSP® NREMR® CAHSO® NFPA-3000 Program Specialist
Active Risk Survival, Inc.
Salisbury, Maryland
410-430-1485
---

top previous next

2. Re: Active Shooter Preparedness

Reply to Group Online | Reply to Sender Online



Apr 25, 2023 9:42 AM
Gerald G Wilkins

Thank you for taking time to read the POETE summary I posted. With the liability associated with Hostile Events in the workplace failure to plan is not an option or defense. FEMA established Incident Command for dealing with the challenges associated with wildfires on the West Coast back in the late 60's. Incident Command is now the standard for responding to any "All Hazard" in the US and many countries around the world. When considering how to conduct a Threat Assessment the THIRA/SPR model which is covered in the FEMA CPG201 provides guidance in Threat Assessment process and assist in determining the GAPS by conducting an Stakeholder Preparedness Review (SPR). Planning and running drills can be done by following the guidance available thru Homeland Security Exercise and Evacuation Program (HSEEP). There are many "open source" documents that can assist in building resilience for any facility against losses and liability. Following industry "Best Practice" can prove to be a power tool for improving overall outcomes of catastrophic events.

Jerry G Wilkins, PSP® NREMR® CAHSO® NFPA-3000 Program Specialist
Active Risk Survival, Inc.
Salisbury, Maryland
410-430-1485

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 24 Apr, 2023 21:23
From: Nishith Agarwal
Subject: Active Shooter Preparedness

Dear Gerald,

Nicely summed up and certainly of a great value..

Regards

[Nishith] [Agarwal] [CPP]
[Raxa Security services Ltd]
[Head Training & Recruitment]
[Military Veteran]
[India]

top previous next

3. Re: Active Shooter Preparedness

Reply to Group Online | Reply to Sender Online

Apr 25, 2023 10:11 AM
Gerald G Wilkins

Thank you for taking time to read the summary I posted. If you take a minute and analyze the formula below you can come up with some very insightful questions.

Risk Equation

R= Risk Outcome/Probability
T= What could Happen
V= What have we done or not done to protect our facility
I= What impact could this event have on our facility/people/reputation/share value
C= Countermeasures People/Process/Technology

Jerry G Wilkins, PSP® NREMR® CAHSO® NFPA-3000 Program Specialist
Active Risk Survival, Inc.
Salisbury, Maryland
410-430-1485

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 25 Apr, 2023 09:14
From: Alan Cranfill
Subject: Active Shooter Preparedness

Hi Gerald,

A great framework.

Thanks!

Alan Cranfill
Director - Health, Safety and Security
Hines Interests LP
Houston TX
United States

top previous next

4. Re: AMAG/Symmetry Latency + Solutions

Reply to Group Online Reply to Sender Online

Apr 25, 2023 8:12 AM
Michael Korn

From time to time we experience lags. We are still using using 8.1 so I guess it's part of the reason why there are issues.

Michael Korn APP
Director of Public Safety
Borough of Manhattan Community College
New York NY

United States

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 24 Apr, 2023 16:39
From: J Downs
Subject: AMAG/Symmetry Latency + Solutions

Hello,

I was curious if any one else experiences significant delays using AMAG/Symmetry and if they have found any solutions for improving the speed.

Thanks for your time!

J Downs

J Downs
Sr Manager Global Security Programs
Lamb Weston
Eagle ID
United States
---

top previous next

5. Re: AMAG/Symmetry Latency + Solutions

Reply to Group Online | Reply to Sender Online

Apr 25, 2023 2:20 PM
Matthew J Underwood

Depending on the size of your system, it could be a number of

factors. Are you seeing lags with real time activity, trigger commands etc.? Or is it just laggy and sluggish to user input?

One of the first things to look at is the server architecture.

Matthew Underwood, MA, PSP, CHSS
Supervisor- System Engineer- Security Technology
Atrium Health
NC

View Thread **Like** **Share Discussion** **Flag as Inappropriate**

Original Message:
Sent: 24 Apr, 2023 16:39
From: J Downs
Subject: AMAG/Symmetry Latency + Solutions

Hello,

I was curious if any one else experiences significant delays using AMAG/Symmetry and if they have found any solutions for improving the speed.

Thanks for your time!

J Downs

J Downs
Sr Manager Global Security Programs
Lamb Weston
Eagle ID
United States

Reply to Group Online | Reply to Sender Online

Apr 25, 2023 8:34 AM
Dwayne M Gulsby

Thanks for the response Kevin and I agree there are many contributors to the current situation. Hopefully we find the path to correct it.

Dwayne Gulsby CPP
Region President
Securitas Security Services USA, Inc
Frederick MD
United States

View Thread | Like | Share Discussion | Flag as Inappropriate

---
Original Message:
Sent: 24 Apr, 2023 15:28
From: Kevin Stranahan
Subject: Law enforcement recruitment

Hello Dwayne

It's a great question. At the local level, I can say that some solutions can involve revisiting police-community partnerships and community relations. I attend my local Compstat meetings very other week and the NHPD is trying to return to many of these initiatives, even despite their short staffing. Much of it can also involve salary equity. In 1997, my starting salary with the NYPD was $27,838. More than twenty five years later, that same starting salary is now only around $42,500. Here in CT, some departments also did away with defined pension plans, which resulted in top talent leaving for other agencies.

The discussion has also (of course) impacted healthcare. In speaking with a CEO from Nuvance Health last week, she admitted to me having to resort to recruiting clinical staff from overseas in order to mitigate attrition in healthcare-critical positions.

Kevin J. Stranahan, CFE, CCI, CPP, PCI, PSP
Director of Risk Management & Safety
Fair Haven Community Health Care
New Haven, CT 06513
203-777-7411

top previous next

7. Re: Law enforcement recruitment

Reply to Group Online | Reply to Sender Online

Apr 25, 2023 9:25 AM
Oscar Odom

Good morning, Dwayne

The 21st century presents new challenges for the law enforcement and public safety community because of the political climate, recent events and the COVID-19 Pandemic. The law enforcement and public safety community must adapt and improvise if we are to survive. First, we must identify the issues that impact those that we are trying to recruit/new generation. Second, Student loan/debt repayments and forgiveness programs are hot topics of debate. Third, The new generation is looking for room to grow/climb the ladder.

Moreover, the following can be marketed to the new generation;

1) "Tuition Reimbursement" coupled with "Room for Advancement" may be a motivating factor for the new generation,

2) Four (4) day work weeks can be marketed as work life balance,

3) Pensions

The following recommendations may assist with negative perceptions, job security, and make the profession more attractive to the new generation!

Dr. Oscar Odom III J.D., Ed.D.
Vice President/CSO of Security
Brooklyn Navy Yard Development Corporation
Brooklyn New York
USA

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 24 Apr, 2023 14:04
From: Dwayne M Gulsby
Subject: Law enforcement recruitment

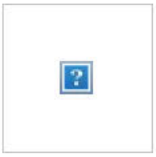
Police departments are coping with critical staffing shortages and struggling to fill their ranks. Which leaves those serving to work long hours and extra overtime to cover for the shortages.
The main reasons for the recruitment and retention crisis are related to multiple social and political forces, including generational differences and a negative perception of policing. Just about every police department is looking for the same group of talented motivated individuals.
How do we turn the tide and shake off the negative perception to make the profession attractive to a new generation? Or are we at a new stage that must be adapted to with lower resources, less services and longer wait times?

Dwayne Gulsby CPP
Region President
Securitas Security Services USA, Inc
Frederick MD
United States
---

top previous next

8. Re: Law enforcement recruitment

Reply to Group Online | Reply to Sender Online



Apr 25, 2023 12:06 PM
Dwayne M Gulsby

Great points Dr. Odom especially with the 4 day work week and pensions!

Dwayne Gulsby CPP
Region President
Securitas Security Services USA, Inc
Frederick MD
United States

View Thread | Like | Share Discussion | Flag as Inappropriate

---
Original Message:
Sent: 25 Apr, 2023 09:24
From: Oscar Odom
Subject: Law enforcement recruitment

Good morning, Dwayne

The 21st century presents new challenges for the law enforcement and public safety community because of the political climate, recent events and the COVID-19 Pandemic. The law enforcement and public safety community must adapt and improvise if we are to survive. First, we must identify the issues that impact those that we are trying to recruit/new generation. Second, Student loan/debt repayments and forgiveness programs are hot topics of debate. Third, The new generation is looking for room to grow/climb the ladder.

Moreover, the following can be marketed to the new generation;

1) "Tuition Reimbursement" coupled with "Room for Advancement" may be a motivating factor for the new generation,

2) Four (4) day work weeks can be marketed as work life balance,

3) Pensions

> The following recommendations may assist with negative perceptions, job security, and make the profession more attractive to the new generation!
>
> ---
> Dr. Oscar Odom III J.D., Ed.D.
> Vice President/CSO of Security
> Brooklyn Navy Yard Development Corporation
> Brooklyn New York
> USA

top previous next

9. Re: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

Reply to Group Online | Reply to Sender Online



Apr 25, 2023 1:40 AM
Charles Jasper

Hey David, if I may chime in here

1. First and foremost, depending on the state or municipality these HOAs are in, people who are victims of crime or in traffic accidents outside these areas will subpoena the HOA for the footage, and when the camera is nonexistent, it opens up a can of worms nobody wants to deal with. In my corporate security days, that was a huge issue with some of our tenants. Additionally, there's a communication issue with the neighborhood. Residents need to know that these cameras either are, or are not proactively monitored (most likely the latter) and that they're for use in common area only. Furthermore, the cameras MUST NOT be capable, in any way, of violating the privacy of people in their own homes.
2. Correct, very few buildings or neighborhoods I've looked at have even remotely sufficient cameras and video monitoring systems, and they're just haphazardly thrown out there.
3. LPRs or LPCs have another privacy issue, and should only be used on gated communities.

Last but not least, signage! Clear signage that tells passersby they may be recorded by the system is a must.

Charles Jasper
Founder & Co-President
C&C Security Consultants, Inc.
West Hollywood CA
United States

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 22 Apr, 2023 16:10
From: David Olmstead
Subject: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

A hot topic for many Neighborhood Homeowner Associations (HOAs) is the deterrent value of surveillance cameras at the entrance/exit to the HOA neighborhood. The questions are usually framed in terms of non-operating (i.e., fake) cameras being the most inexpensive but may carry liability issues, real cameras that provide low quality video of little evidentiary value in capturing and convicting a perpetrator, versus something like the more expensive License Plate Cameras (LPCs) that require well planned placement to actually capture the License Plate (sometimes requiring more cameras than originally anticipated and therefore at an increased cost because of performance design requirements).
I have even heard HOA members claim that since there was a break-in, if the HOA does not do something to improve security and there is another break-in the HOA can be sued for failing to act to improve security. I dismissed this as overreach. Even though an HOA is incorporated, it is different than a business that does have an obligation to act because they are inviting people into their establishment. Adding security to a public road is not an obligation of the HOA.
It is over 20 years since I considered this issue, so I am looking for any recent studies or standards.
My previous assessments and current opinion generally come down to the following:
1. Fake cameras are generally a bad idea because they do not actually provide anything of value and carry a liability issue (even if small, it outweighs the nearly nonexistent deterrent value).
2. Back when I previously looked at this issue, the average camera systems gave low quality images, and the recordings (often analog) made things even worse. The evidentiary value might point law enforcement in a direction (e.g., color of vehicle, maybe vehicle make

and model, etc.). Unless the surveillance system was well designed, details were hard to observe.

3. Today we have LPCs that can easily capture the license number (sometimes requiring vehicle information for definitive capture) and a toll bill is sent to the vehicle owner. This indicates a high evidentiary value, but again requires good system design. Its deterrent value will follow a history of effective use by law enforcement. If it is not effective in identifying perpetrators (or at least their vehicles) its deterrent value will be low just as it is with old analog cameras.

I still believe this today, and that the ultimate answer is in the cost/benefit. Do the HOA "members" want the benefit promised at the cost to achieve it.

Thank you all, in advance, for your time at weighing in.

David Olmstead
CPP, FL, United States
---

top previous next

10. Re: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

Reply to Group Online | Reply to Sender Online

Apr 25, 2023 4:54 AM
Anthony Beattie

There are current studies that show cameras are no deterrent to crime, some show decreasing deterrence with offender age (ie, teenagers are the least deterred).
Apprehension, however, IS effective. So, as part of complete security package, cameras benefits are based off their capabilities.

Anthony Beattie
ACAP - Solutions for School Safety
Grand Ledge MI

United States

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 22 Apr, 2023 16:10
From: David Olmstead
Subject: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

A hot topic for many Neighborhood Homeowner Associations (HOAs) is the deterrent value of surveillance cameras at the entrance/exit to the HOA neighborhood. The questions are usually framed in terms of non-operating (i.e., fake) cameras being the most inexpensive but may carry liability issues, real cameras that provide low quality video of little evidentiary value in capturing and convicting a perpetrator, versus something like the more expensive License Plate Cameras (LPCs) that require well planned placement to actually capture the License Plate (sometimes requiring more cameras than originally anticipated and therefore at an increased cost because of performance design requirements).
I have even heard HOA members claim that since there was a break-in, if the HOA does not do something to improve security and there is another break-in the HOA can be sued for failing to act to improve security. I dismissed this as overreach. Even though an HOA is incorporated, it is different than a business that does have an obligation to act because they are inviting people into their establishment. Adding security to a public road is not an obligation of the HOA.
It is over 20 years since I considered this issue, so I am looking for any recent studies or standards.
My previous assessments and current opinion generally come down to the following:
1. Fake cameras are generally a bad idea because they do not actually provide anything of value and carry a liability issue (even if small, it outweighs the nearly nonexistent deterrent value).
2. Back when I previously looked at this issue, the average camera systems gave low quality images, and the recordings (often analog) made things even worse. The evidentiary value might point law enforcement in a direction (e.g., color of vehicle, maybe vehicle make and model, etc.). Unless the surveillance system was well designed, details were hard to observe.
3. Today we have LPCs that can easily capture the license number (sometimes requiring vehicle information for definitive capture) and a toll bill is sent to the vehicle owner. This indicates a high evidentiary value, but again requires good system design. Its deterrent value will follow a history of effective use by law enforcement. If it is not effective in identifying perpetrators (or at least their vehicles) its deterrent value will be low just as it is with old analog cameras.
I still believe this today, and that the ultimate answer is in the cost/benefit. Do the HOA

"members" want the benefit promised at the cost to achieve it.
Thank you all, in advance, for your time at weighing in.

David Olmstead
CPP, FL, United States
---

top previous next

11. Re: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

Reply to Group Online | Reply to Sender Online

Apr 25, 2023 5:39 AM
K. Campbell

There is likely little to no deterrent value of cameras at the entrance/exist of a neighborhood.

I recently completed a risk assessment for an HOA (a large subdivision) and one of the main purposes of the assessment was to determine the deterrent value of the leased camera system. All but one of the installations were placed at the four entrances/exits to the subdivision. Based on police crime data for the subdivision, I found no evidence the camera system had deterrent value. In fact, when the HOA later requested I use crime data from before the camera system was installed (for a total of 11 years of crime data) to compare crime rates before and after the camera system's installation, I found that crime in the subdivision *increased* after the cameras' installation.

These findings are consistent with studies in the U.S. and elsewhere. The deterrent value of community cameras, including cameras owned and operated by police, is mixed at best. In some cases of police camera systems, crime *increased* after their installation. Some sources, including a DoJ-sponsored study:

1. University of Tennessee, Municipal Technical Advisory Service (MTAS), September 2016, *Is There Empirical Evidence that Surveillance Cameras Reduce Crime?* www.mtas.tennessee.edu/knowledgebase/...
2. The Urban Institute. September 2011, *Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention.* cops.usdoj.gov/RIC/Publications/cops-w0614-pub.pdf
3. Measuring the Effects of Video Surveillance on Crime in Los Angeles. CRB-08-007. Sacramento, CA: California Research Bureau. www.library.ca.gov/wp-content/uploads/crb-reports/....

Some folks in this discussion have mentioned these camera systems' value in *investigating* crime. For one, most wide-area cameras inherently have a low resolution due to their small focal lens. This results in resolution that's usually not suitable for recognition or identification of suspects. Most camera salespeople don't disclose these limitations to HOAs. It's even worse at night. In my risk assessment I included a real-world example of a video capture from the system at night after a serious crime. You can tell only that the subjects were two humans, even when they were only 30 feet away from the camera.

Finally, I find that homeowners have a significant overreliance and overconfidence in these community/neighborhood camera systems (again, many aren't aware of these cameras' limitations), and many homeowners take little, if any, responsibility for their own safety and security (home exterior lighting, landscaping, individual camera and alarm systems, etc.). In this recent risk assessment, I saw a direct correlation between several car thefts and non-existent landscaping (i.e., views of the street was completely blocked by tree branches and shrubbery).

K. Campbell, CBCP, CPP
www.linkedin.com/in/kcampbe

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 22 Apr, 2023 16:10
From: David Olmstead

Subject: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

A hot topic for many Neighborhood Homeowner Associations (HOAs) is the deterrent value of surveillance cameras at the entrance/exit to the HOA neighborhood. The questions are usually framed in terms of non-operating (i.e., fake) cameras being the most inexpensive but may carry liability issues, real cameras that provide low quality video of little evidentiary value in capturing and convicting a perpetrator, versus something like the more expensive License Plate Cameras (LPCs) that require well planned placement to actually capture the License Plate (sometimes requiring more cameras than originally anticipated and therefore at an increased cost because of performance design requirements).

I have even heard HOA members claim that since there was a break-in, if the HOA does not do something to improve security and there is another break-in the HOA can be sued for failing to act to improve security. I dismissed this as overreach. Even though an HOA is incorporated, it is different than a business that does have an obligation to act because they are inviting people into their establishment. Adding security to a public road is not an obligation of the HOA.

It is over 20 years since I considered this issue, so I am looking for any recent studies or standards.

My previous assessments and current opinion generally come down to the following:

1. Fake cameras are generally a bad idea because they do not actually provide anything of value and carry a liability issue (even if small, it outweighs the nearly nonexistent deterrent value).
2. Back when I previously looked at this issue, the average camera systems gave low quality images, and the recordings (often analog) made things even worse. The evidentiary value might point law enforcement in a direction (e.g., color of vehicle, maybe vehicle make and model, etc.). Unless the surveillance system was well designed, details were hard to observe.
3. Today we have LPCs that can easily capture the license number (sometimes requiring vehicle information for definitive capture) and a toll bill is sent to the vehicle owner. This indicates a high evidentiary value, but again requires good system design. Its deterrent value will follow a history of effective use by law enforcement. If it is not effective in identifying perpetrators (or at least their vehicles) its deterrent value will be low just as it is with old analog cameras.

I still believe this today, and that the ultimate answer is in the cost/benefit. Do the HOA "members" want the benefit promised at the cost to achieve it.

Thank you all, in advance, for your time at weighing in.

David Olmstead
CPP, FL, United States

---

top previous

12. Re: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

Reply to Group Online | Reply to Sender Online

Apr 25, 2023 7:00 AM
Salvatore A D'Agostino

Thanks for the message about Signage and Notice, often lacking and a focus of ours as well as providing the operational capabilities associated with the Notice in terms of information and response.

Salvatore D'Agostino
CEO
IDmachines
Brookline MA
United States

View Thread Like Share Discussion Flag as Inappropriate

Original Message:
Sent: 24 Apr, 2023 14:16
From: Jon Polly
Subject: Deterrent value of Cameras at the entrance/exit of a Neighborhood.

Hello,

I am a security technology consultant with a background in policing and citywide surveillance.

Reasons for cameras in HOAs run the gambit, from those that want to "see" everything going on in the neighborhood to those that don't want to be "watched". Common areas such as clubhouses and entryways are typical locations where A) the HOA owns, and B) where crime is possible to happen; i.e. open areas where crowds can gather. This makes a good place to put cameras, but these are not

deterrents to criminals as noted by @Michael A Silva.

HOAs also tend to make decisions based on cost. Many times, the cameras that are installed are of fair quality cameras based solely on price and not quality. The outcome is that even in near-perfect conditions; the cameras are successful to get an image, but not one detailed enough to provide recognition or identification of a person. Recognition here is not a facial biometric, although it could be. Cameras should be placed in the clubhouse, areas where crowds congregate, and to view areas where someone could get hurt, i.e. playgrounds and pools. While there may be a function of deterrence, this is more for an insurance requirement in the event of damage or injury.

License Plate Capture (LPC) as noted has been marginally successful in HOAs. Most LPC cameras are standard 1080p (2MP) cameras running an Optical Character Recognition (OCR) software analytic. Unlike traditional Automated License Plate Recognition (ALPR) cameras which can run upwards of $25K before installation; LPC cameras are significantly cheaper at around $2K - $5K per camera. The reduced cost typically comes with reduced accuracy, using a traditional CCTV imager vs. a black-and-white imager. The LPC works best with slower speeds, in areas of good lighting, and in a closer field of view. Most HOAs have a slow-speed entrance, with plenty of lighting, and a short field of view for the camera to work. These are best-case scenarios and still, most LPCs have an 85% or less accuracy. Here are a couple of articles I have written on the subject of LPC cameras (www.securityinfowatch.com/video-surveillance/...) and (www.securityinfowatch.com/video-surveillance/...)

Property Management companies have little say in what systems they install but may point them to a system integrator. HOAs and Property Management company contracts fluctuate with the changing of the HOA board.

A few notes of specific things to help HOAs avoid problems others have faced.

Policy
To be successful, putting cameras in an HOA requires a well-crafted policy on how long the data will be retained, as well as how the data will be handled. Admirably, many HOAs want to share LPC and camera data with the local police department through a public-private partnership (P3). This is a great idea, however, there must be a defined policy in place on what and how that data is shared, so that those in the HOA who have an expectation of privacy do in fact have that privacy. Not that they are doing illegal actions, but that they give informed consent. The policy should be reviewed by a legal expert to ensure that the HOA is legal in their actions to share data and that the HOA has a signed Memorandum of Understanding (MOU) with any law enforcement department they are sharing video with; even if a board member is a local law enforcement officer.

Depending on the types of analytics, i.e. facial recognition; a policy with an expressed opt-in by every resident and guest would be required.

Signage

Signage is critical. Signage is a public notice to all entering the property that they are under surveillance and that there is a limited expectation of privacy. It should be affixed to any LPC camera as well as any common areas that are in a camera field of view.

Lighting
Most cameras require a certain amount of ambient light. Law enforcement agencies want only color cameras, even cameras that have IR filters to turn black and white when the lighting is too low don't work because the person and their clothing are not identifiable. Installing cameras without the right amount of lighting is going to waste good money on a system that won't provide the detail desired. Better quality cameras may require less ambient light; the better the lighting, the better the camera image. LPC cameras specifically require a significant amount of ambient light.

Long Term Contracts
Speaking above about LPC cameras, buyer beware. Some of the LPC camera manufacturers (I won't disclose names), sell cameras at a simple yearly price but with required multi-year commitments. These multi-year commitments lock the HOA board in, even if the board changes. Many of these offer cloud services which again points back to data and data retention, locking the HOA board into needing to keep the service because of the data retained. As stated above, LPC cameras can be great tools, but HOAs can become a target of their own want to eliminate crime.

Security isn't just cameras
The term defense in depth still applies here. CPTED strategies, fencing, etc. are all still valid and should be considered as part of the security of the HOA, from multi-tenant buildings to housing neighborhoods.

Jon Polly, PSP, SICC, IC3PM
Chief Solutions Officer
ProTecht Solutions Partners, LLC
(704) 759-6837
Charleston SC
United States
www.linkedin.com/in/JonPolly
www.protechtsolutionspartners.com

You are subscribed to "Open Forum" as paul.upton@pol.state.ma.us. To change your subscriptions, go to My Subscriptions.

From: Cleve Daniels
To: Pack, Noah (POL)
Subject: RE: [External] LPR MOU
Date: Wednesday, May 31, 2023 2:59:17 PM

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

Sgt Pack,

Hope all is well. Just wanted to check in regarding the State's ALPR system. We have been trying to query the system several times over the past week but are not getting any data back. Is the system down or have there been any changes?

Thanks as always.

Deputy Chief Cleve G. Daniels
Dennis Police Department
90 Bob Crowell Road
South Dennis, MA 02660
Office: (774) 352-1522
Fax: (774) 352-1442
cdaniels@town.dennis.ma.us

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Sent: Tuesday, March 28, 2023 12:19 PM
To: Cleve Daniels <cdaniels@town.dennis.ma.us>
Subject: [External] LPR MOU

CAUTION: This email originated from outside your organization. Exercise caution when opening attachments or clicking links, especially from unknown senders.

Chief Daniels,

Attached is a signed copy of the ALPR MOU for your agency's records.

Respectfully,

Noah

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

This electronic message is confidential and intended for the named recipient only. Any dissemination, disclosure or distribution of the contents of this communication is unlawful and prohibited. If you have received this message in error, please contact the sender by return email or telephone and delete the copy you received. Thank you.

From: Melander, John (EPS)
To: Kwon, Gina K. (EPS)
Cc: Staples, Jennifer (POL); Terrey, Susan (EPS); Walker, Suleyken (EPS)
Subject: RE: ALPR Cameras and FLOCK
Date: Thursday, September 7, 2023 7:39:24 AM

Gina,

Happy to connect with you about this and cover next week.

Thanks,

John

From: Kwon, Gina K. (EPS) <Gina.K.Kwon@mass.gov>
Sent: Wednesday, September 6, 2023 5:24 PM
To: Melander, John (EPS) <John.Melander@mass.gov>
Cc: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>; Walker, Suleyken (EPS) <Suleyken.Walker@mass.gov>
Subject: Re: ALPR Cameras and FLOCK

Sorry, I'm away next week. I can fill in eopss team with my convos with MassDOT before I leave.

Sent from my iPhone

> On Sep 6, 2023, at 12:57 PM, Melander, John (EPS) <John.Melander@mass.gov> wrote:
>
> Hi Jen,
>
> Either day works for me.
>
> Thanks,
>
> John
>
> ---
>
> **From:** Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>
> **Sent:** Wednesday, September 6, 2023 12:46 PM
> **To:** Kwon, Gina K. (EPS) <Gina.K.Kwon@mass.gov>; Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>; Walker, Suleyken (EPS) <Suleyken.Walker@mass.gov>; Melander, John (EPS) <John.Melander@mass.gov>
> **Subject:** ALPR Cameras and FLOCK
>
> Hi All:

Could we schedule a time next week to discuss with Colonel Cyr and the ALPR folks MSP purchasing a FLOCK ALPR Camera subscription? Not FLOCK cameras, but a subscription in order to access data.

Sue, I included you because you were originally involved in ALPR cameras, but feel free to bow out. ☺

Let me know if maybe Tuesday or Wednesday work.

Thanks!!

Jennifer M. Staples
Chief Legal Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Tel: (508) 820-2307
G.L. c. 4.sec. 7.cl 26 (n)(security)


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: Melander, John (EPS)
To: Pack, Noah (POL)
Subject: RE: ALPR Policy
Date: Friday, October 13, 2023 1:50:50 PM

Hi Sgt.,

The *McCarthy* case references "EOPSS's" ALPR policy. Any chance you have it? I've never seen one. I'm wondering if we delegated to MSP? Appreciate an insights you may have.

Thanks,

John

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Thursday, October 12, 2023 9:49 PM
To: Melander, John (EPS) <John.Melander@mass.gov>
Subject: Re: ALPR Policy

Hi John,

To ensure that the Department has an up-to-date policy that reflects current law, best practices, and our public safety priorities, there were a number of changes in this update. The document was also reorganized, so a version to version comparison would not be particularly helpful. Here are some of the highlights:

Authorized/Prohibited Uses

- Revised authorized uses to emphasize the Department's prioritization of ALPR use for serious public safety and homeland security matters
- Added authorized use for motor vehicle pursuit follow-up, due to frequent pursuit termination for public safety and de-escalation
- Added restriction against use for immigration enforcement

Legal Considerations

- Added section on legal considerations to address McCarthy case law

Search Procedures

- Revised section to provide clear guidelines on search justification & documentation
- Added requirement to limit searches to be reasonable and consistent with the geographic and temporal needs of the incident or investigation
- Added authorization for Fusion Center staff to deny overly intrusive or improper requests

Manual Hotlist Entries

- Reduced maximum time from 1 year to 30 days, with built-in automatic expiration to prevent error or misuse
- Added requirement for supervisory approval, unless exigent circumstances
- Added cautionary notice to give special attention to rental and short-term use vehicles and incidents that may be quickly resolved

Use of Non-Departmental ALPR Systems:

- Added restrictions on access to outside systems
- Added cautionary notice on different technology/retention of other systems

Other Miscellaneous Updates:

- Added requirement that user training includes discussion of privacy considerations and best practices
- Improved section on verifying LPR hits prior to taking enforcement action
- Added that LPR data does not include any video or audio recordings or intentional photos of persons
- Added notice/requirement for time verification protocols to ensure that accurate data can be confirmed and inaccurate data can be identified

Please let me know if I can provide anything further.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Cell: [redacted]

From: Melander, John (EPS) <John.Melander@mass.gov>
Sent: Thursday, October 12, 2023 2:42 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: ALPR Policy

Hi Noah,

Could you tell me what part of the attached policy was added/amended in June? I think the “Use of

Non-Departmental ALPR System" was added, so just wondering if anything else changed in June. Maybe you have a redline?

Thanks!

John Melander
Deputy General Counsel
Executive Office of Public Safety and Security
One Ashburton Place, Suite 2133
Boston, MA 02108
G L. c. 4.sec. 7.cl.26 (n)(security)

From: Melander, John (EPS)
To: Pack, Noah (POL)
Subject: RE: ALPR Policy
Date: Thursday, October 12, 2023 9:51:37 PM

Got it. This is helpful. Thanks, Sgt.

John

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Thursday, October 12, 2023 9:49 PM
To: Melander, John (EPS) <John.Melander@mass.gov>
Subject: Re: ALPR Policy

Hi John,

To ensure that the Department has an up-to-date policy that reflects current law, best practices, and our public safety priorities, there were a number of changes in this update. The document was also reorganized, so a version to version comparison would not be particularly helpful. Here are some of the highlights:

Authorized/Prohibited Uses

- Revised authorized uses to emphasize the Department's prioritization of ALPR use for serious public safety and homeland security matters
- Added authorized use for motor vehicle pursuit follow-up, due to frequent pursuit termination for public safety and de-escalation
- Added restriction against use for immigration enforcement

Legal Considerations

- Added section on legal considerations to address McCarthy case law

Search Procedures

- Revised section to provide clear guidelines on search justification & documentation
- Added requirement to limit searches to be reasonable and consistent with the geographic and temporal needs of the incident or investigation
- Added authorization for Fusion Center staff to deny overly intrusive or improper requests

Manual Hotlist Entries

- Reduced maximum time from 1 year to 30 days, with built-in automatic expiration to prevent error or misuse

- Added requirement for supervisory approval, unless exigent circumstances
- Added cautionary notice to give special attention to rental and short-term use vehicles and incidents that may be quickly resolved

Use of Non-Departmental ALPR Systems:

- Added restrictions on access to outside systems
- Added cautionary notice on different technology/retention of other systems

Other Miscellaneous Updates:

- Added requirement that user training includes discussion of privacy considerations and best practices
- Improved section on verifying LPR hits prior to taking enforcement action
- Added that LPR data does not include any video or audio recordings or intentional photos of persons
- Added notice/requirement for time verification protocols to ensure that accurate data can be confirmed and inaccurate data can be identified

Please let me know if I can provide anything further.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
G.L. c. 4.sec. 7.cl.26 (n)(security)

From: Melander, John (EPS) <John.Melander@mass.gov>
Sent: Thursday, October 12, 2023 2:42 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: ALPR Policy

Hi Noah,

Could you tell me what part of the attached policy was added/amended in June? I think the "Use of Non-Departmental ALPR System" was added, so just wondering if anything else changed in June. Maybe you have a redline?

Thanks!

John Melander
Deputy General Counsel
Executive Office of Public Safety and Security
One Ashburton Place, Suite 2133
Boston, MA 02108
G L. c. 4.sec. 7.cl.26 (n)(security)

From: Melander, John (EPS)
To: Pack, Noah (POL)
Subject: RE: ALPR Policy
Date: Friday, October 13, 2023 2:47:02 PM

Agreed. I'm pretty positive we don't have one. But that's fine, we have yours. Making progress on this btw, should have some news soon.

Thanks for clarifying,

John

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Friday, October 13, 2023 2:08 PM
To: Melander, John (EPS) <John.Melander@mass.gov>
Subject: Re: ALPR Policy

Hi John,

I am also unaware of any such EOPSS document. If it did exist, it predates my involvement. I think they most likely mean either MSP's policy or a DCJIS policy. To that end, the only DCJIS document I'm aware of that relates to this is the public safety information sharing policy, which does not appear to reference LPR specifically.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

From: Melander, John (EPS) <John.Melander@mass.gov>
Sent: Friday, October 13, 2023 1:50:46 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: RE: ALPR Policy

Hi Sgt.,

The *McCarthy* case references "EOPSS's" ALPR policy. Any chance you have it? I've never seen one. I'm wondering if we delegated to MSP? Appreciate an insights you may have.

Thanks,

John

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Thursday, October 12, 2023 9:49 PM
To: Melander, John (EPS) <John.Melander@mass.gov>
Subject: Re: ALPR Policy

Hi John,

To ensure that the Department has an up-to-date policy that reflects current law, best practices, and our public safety priorities, there were a number of changes in this update. The document was also reorganized, so a version to version comparison would not be particularly helpful. Here are some of the highlights:

Authorized/Prohibited Uses

- Revised authorized uses to emphasize the Department's prioritization of ALPR use for serious public safety and homeland security matters
- Added authorized use for motor vehicle pursuit follow-up, due to frequent pursuit termination for public safety and de-escalation
- Added restriction against use for immigration enforcement

Legal Considerations

- Added section on legal considerations to address McCarthy case law

Search Procedures

- Revised section to provide clear guidelines on search justification & documentation
- Added requirement to limit searches to be reasonable and consistent with the geographic and temporal needs of the incident or investigation
- Added authorization for Fusion Center staff to deny overly intrusive or improper requests

Manual Hotlist Entries

- Reduced maximum time from 1 year to 30 days, with built-in automatic expiration to prevent error or misuse
- Added requirement for supervisory approval, unless exigent circumstances
- Added cautionary notice to give special attention to rental and short-term use vehicles and incidents that may be quickly resolved

Use of Non-Departmental ALPR Systems:

- Added restrictions on access to outside systems
- Added cautionary notice on different technology/retention of other systems

Other Miscellaneous Updates:

- Added requirement that user training includes discussion of privacy considerations and best practices

From: Michael Roth
To: Pack, Noah (POL)
Cc: jtedona@neology.net; gnavarrete@neology.mx; ipadilla@neology.mx; mroth
Subject: Re: Audit Request for Old Boss3. [ref:_00D1N1wyfS._5003l1WpsKj:ref]
Date: Wednesday, June 21, 2023 12:07:12 PM

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

Hello all, I have this case file under my name and wanted to make sure if this was still something that still needs addressed or was resolved?

Regards, M.Roth

---------- Original Message ----------
From: Pack, Noah [noah.pack@state.ma.us]
Sent: 4/26/2023 11:40 AM
To: ipadilla@neology.mx
Cc: jtedona@neology.net; alpr_support@neology.net; gnavarrete@neology.mx; mroth@neology.net
Subject: Re: Audit Request for Old Boss3. [ref:_00D1N1wyfS._5003l1WpsKj:ref]

The Boss3 database is no longer online. The only potential source I'm aware of for this would be if audit tables had been backed up during the transition. If that is not available, I don't believe this data would exist anywhere else.

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

From: Israel Padilla Sánchez <ipadilla@neology.mx>
Sent: Wednesday, April 26, 2023 10:05 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: John Tedona <jtedona@neology.net>; ALPR_Support <ALPR_Support@neology.net>; Giovanni Navarrete Araiza <gnavarrete@neology.mx>; mroth <mroth@neology.net>
Subject: Re: Audit Request for Old Boss3. [ref:_00D1N1wyfS._5003l1WpsKj:ref]

CAUTION: This email originated from a sender outside of the 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 all,

Yes, as John mentioned, it is desirable to narrow the search parameters. We have the database files separated in time ranges in AWS. We will need to start a SQL Server instance in the cloud and attach the correct set of files according to the date. I think we didn't back up the audits table, only the reads and images.

As Michael mentioned, if you still have the BOSS3 DB in place, we can help searching in the audits table.

I'll review the files and let you know what I find.

Regards
Israel

Sent from my iPhone

> On 26 Apr 2023, at 8:00, Michael Roth <mroth@neology.net> wrote:
>
> ?

Hey Noah, it's possible if someone still has access to the old system and if Justifications was enabled at the time of the query. As for BOSS4 if that data had been transferred during the migration it is definitely gone due to the current retention policy on data and system audits.

Michael Roth

Application Development

Mobile: + 513 [redacted]

Email: mroth@neology.net

13520 Evening Creek Dr E #460,

San Diego, CA 92128

www.neology.net

[Image is no longer available]
[Image is no longer available]

***Customer Support& Sales*:** (833) PIPS-LPR or (833) 747-7577

Alpr_support@neology.net – Technical Service/Repair

Alpr@neology net - Sales Inquiry

From: John Tedona <jtedona@neology.net>
Sent: Wednesday, April 26, 2023 9:17 AM
To: Pack, Noah (POL) <noah.pack@state.ma.us>; ALPR_Support <ALPR_Support@neology.net>
Cc: Michael Roth <mroth@neology.net>; Israel Padilla Sánchez <ipadilla@neology.mx>
Subject: RE: Audit Request for Old Boss3

Hi Noah,

Please forward additional information if available to narrow down the search criteria e.g. the user name, date, plate number

Thanks,

John Tedona

Sales Manager

Mobile: 201-[redacted]

Email: jtedona@neology.net

13520 Evening Creek Drive North, Suite 460

San Diego, CA 92128

www.neology.net

[Image is no longer available][Image is no longer available]

***Customer Support& Sales*:** (833) 747-7LPR or (833) 747-7577

Alpr_support@neology.net – Technical Service/Repair

Alpr@neology net - Sales Inquiry

https://www.policegrantshelp.com/neology-grant-assistance/ - Grant Assistance

---

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Sent: Monday, April 24, 2023 3:27 PM
To: ALPR_Support <ALPR_Support@neology.net>
Cc: John Tedona <jtedona@neology.net>; Michael Roth <mroth@neology.net>; Israel Padilla Sánchez <ipadilla@neology.mx>
Subject: Audit Request for Old Boss3

We received a request from a partner agency looking to determine the search parameters that were used for what sounds like search of the Boss3 system on a read from 2020.

Is there any way to access that information, given the age of the request and the change in software/server?

Respectfully,

Noah

Sergeant Noah H. Pack

Massachusetts State Police

Division of Homeland Security and Preparedness

Office of the Division Commander



From: Pack, Noah (POL)
To: mroth
Subject: Re: Audit Request for Old Boss3. [ref:_00D1N1wyfS._5003l1WpsKj:ref]
Date: Wednesday, June 21, 2023 12:57:16 PM

This can be closed. Thanks Mike.

From: Michael Roth <mroth@neology.net>
Sent: Wednesday, June 21, 2023 12:05 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: jtedona@neology.net <jtedona@neology.net>; gnavarrete@neology.mx <gnavarrete@neology.mx>; ipadilla@neology.mx <ipadilla@neology.mx>; mroth <mroth@neology.net>
Subject: Re: Audit Request for Old Boss3. [ref:_00D1N1wyfS._5003l1WpsKj:ref]

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

Hello all, I have this case file under my name and wanted to make sure if this was still something that still needs addressed or was resolved?

Regards, M.Roth

---------- Original Message ----------
From: Pack, Noah [noah.pack@state.ma.us]
Sent: 4/26/2023 11:40 AM
To: ipadilla@neology.mx
Cc: jtedona@neology.net; alpr_support@neology.net; gnavarrete@neology.mx; mroth@neology.net
Subject: Re: Audit Request for Old Boss3. [ref:_00D1N1wyfS._5003l1WpsKj:ref]

The Boss3 database is no longer online. The only potential source I'm aware of for this would be if audit tables had been backed up during the transition. If that is not available, I don't believe this data would exist anywhere else.

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

From: Israel Padilla Sánchez <ipadilla@neology.mx>
Sent: Wednesday, April 26, 2023 10:05 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: John Tedona <jtedona@neology.net>; ALPR_Support <ALPR_Support@neology.net>; Giovanni Navarrete Araiza <gnavarrete@neology.mx>; mroth <mroth@neology.net>
Subject: Re: Audit Request for Old Boss3. [ref:_00D1N1wyfS._5003l1WpsKj:ref]

CAUTION: This email originated from a sender outside of the 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 all,

Yes, as John mentioned, it is desirable to narrow the search parameters. We have the database files separated in time ranges in AWS. We will need to start a SQL Server instance in the cloud and attach the correct set of files according to the date. I think we didn't back up the audits table, only the reads and images.

As Michael mentioned, if you still have the BOSS3 DB in place, we can help searching in the audits table.

I'll review the files and let you know what I find.

Regards
Israel

Sent from my iPhone

> On 26 Apr 2023, at 8:00, Michael Roth <mroth@neology.net> wrote:
>
> ?

Hey Noah, it's possible if someone still has access to the old system and if Justifications was enabled at the time of the query. As for BOSS4 if that data had been transferred during the migration it is definitely gone due to the current retention policy on data and system audits.

Michael Roth
Application Development

Mobile: + 513 [redacted]
Email: mroth@neology.net

13520 Evening Creek Dr E #460,
San Diego, CA 92128

www.neology.net

[Image is no longer available]
[Image is no longer available]

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

From: John Tedona <jtedona@neology.net>
Sent: Wednesday, April 26, 2023 9:17 AM
To: Pack, Noah (POL) <noah.pack@state.ma.us>; ALPR_Support <ALPR_Support@neology.net>
Cc: Michael Roth <mroth@neology.net>; Israel Padilla Sánchez <ipadilla@neology.mx>
Subject: RE: Audit Request for Old Boss3

Hi Noah,

Please forward additional information if available to narrow down the search criteria e.g. the user name, date, plate number

Thanks,

John Tedona
Sales Manager

Mobile: 201.[redacted]
Email: jtedona@neology.net

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

www.neology.net

[Image is no longer available][Image is no longer available]

***Customer Support& Sales*:** (833) 747-7LPR or (833) 747-7577
Alpr_support@neology.net – Technical Service/Repair
Alpr@neology net - Sales Inquiry
https://www.policegrantshelp.com/neology-grant-assistance/ - Grant Assistance

---

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Sent: Monday, April 24, 2023 3:27 PM
To: ALPR_Support <ALPR_Support@neology.net>
Cc: John Tedona <jtedona@neology.net>; Michael Roth <mroth@neology.net>; Israel Padilla Sánchez <ipadilla@neology.mx>
Subject: Audit Request for Old Boss3

We received a request from a partner agency looking to determine the search parameters that were used for what sounds like search of the Boss3 system on a read from 2020.

Is there any way to access that information, given the age of the request and the change in

software/server?

Respectfully,

Noah

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



From: Giovanni Navarrete Araiza
To: Bradley Feldmann; Pack, Noah (POL)
Cc: Israel Padilla Sánchez; John Tedona; Luke Normington; ALPR_Support; mroth; Enrique Martinez de Velasco; Victor Alan Miranda Cortez; Michell Itallekzi Garcia Garcia; Daniela Geraldine Ponce Calderon
Subject: Re: Boss4 Dashboard
Date: Thursday, May 18, 2023 9:34:51 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.

Good morning.

Let us check and find the most quickly way to fix this.

Giovanni Navarrete

Obtener Outlook para iOS

De: Bradley Feldmann <bfeldmann@neology.net>
Enviado: Thursday, May 18, 2023 7:32:49 AM
Para: Pack, Noah (POL) <noah.pack@state.ma.us>
Cc: Israel Padilla Sánchez <ipadilla@neology.mx>; John Tedona <jtedona@neology.net>; Luke Normington <LNormington@uk.neology.net>; ALPR_Support <ALPR_Support@neology.net>; Michael Roth <mroth@neology.net>; Enrique Martinez de Velasco <emartinez@neology.mx>; Victor Alan Miranda Cortez <vmiranda@neology.mx>; Michell Itallekzi Garcia Garcia <mgarcia@neology.mx>; Daniela Geraldine Ponce Calderon <dponce@neopartners.mx>; Giovanni Navarrete Araiza <gnavarrete@neology.mx>
Asunto: Re: Boss4 Dashboard

Giovanni and Israel: please advise soonest
How can we get Noah's team back please?
Should we revert to previous version while we investigate

Sent from my iPhone

> On May 18, 2023, at 6:25 AM, Pack, Noah (POL) <noah.pack@state.ma.us> wrote:
>
> Good morning,
>
> Following the update, multiple users are reporting that the reports functions do not work and they cannot see any read images.
>
> My administrative account is not experiencing these issues - I can see reads and create reports.

I am troubleshooting this now, but if the update made any changes to user account settings or permissions, please advise so I can get the system working again for the end users.

Respectfully,

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

From: Bradley Feldmann <bfeldmann@neology.net>
Sent: Thursday, May 18, 2023 7:09 AM
To: Israel Padilla Sánchez <ipadilla@neology.mx>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; John Tedona <jtedona@neology.net>; Luke Normington <LNormington@uk.neology.net>
Cc: ALPR_Support <ALPR_Support@neology.net>; mroth <mroth@neology.net>; Enrique Martinez de Velasco <emartinez@neology.mx>; Victor Alan Miranda Cortez <vmiranda@neology.mx>; Michell Itallekzi Garcia Garcia <mgarcia@neology.mx>; Daniela Geraldine Ponce Calderon <dponce@neopartners.mx>; Giovanni Navarrete Araiza <gnavarrete@neology.mx>
Subject: Re: Boss4 Dashboard

CAUTION: This email originated from a sender outside of the 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 very much

From: Israel Padilla Sánchez <ipadilla@neology.mx>
Date: Thursday, May 18, 2023 at 12:47 AM
To: Bradley Feldmann <bfeldmann@neology.net>, Pack, Noah (POL) <noah.pack@state.ma.us>, John Tedona <jtedona@neology.net>, Luke Normington <LNormington@uk.neology.net>
Cc: ALPR_Support <ALPR_Support@neology.net>, Michael Roth <mroth@neology.net>, Enrique Martinez de Velasco <emartinez@neology.mx>, Victor Alan Miranda Cortez <vmiranda@neology.mx>, Michell Itallekzi Garcia Garcia <mgarcia@neology.mx>, Daniela Geraldine Ponce Calderon <dponce@neopartners.mx>, Giovanni Navarrete Araiza

<gnavarrete@neology.mx>
Subject: Re: Boss4 Dashboard

Hi all,

BOSS4 is updated to version 59.0.5. The services are performing well. The retention ms is still stopped until I can validate it.

Regards
--
Israel Padilla

From: Bradley Feldmann <bfeldmann@neology.net>
Sent: Wednesday, May 17, 2023 2:54 PM
To: Pack, Noah (POL) <noah.pack@state.ma.us>; Israel Padilla Sánchez <ipadilla@neology.mx>; John Tedona <jtedona@neology.net>; Luke Normington <LNormington@uk.neology.net>
Cc: ALPR_Support <ALPR_Support@neology.net>; Michael Roth <mroth@neology.net>; Enrique Martinez de Velasco <emartinez@neology.mx>; Victor Alan Miranda Cortez <vmiranda@neology.mx>; Michell Itallekzi Garcia Garcia <mgarcia@neology.mx>; Daniela Geraldine Ponce Calderon <dponce@neopartners.mx>; Giovanni Navarrete Araiza <gnavarrete@neology.mx>
Subject: Re: Boss4 Dashboard

Israel: please keep us POSTED regarding the software update. Please ensure goes well. Thanks much, Brad

---

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Date: Wednesday, May 17, 2023 at 1:49 PM
To: Israel Padilla Sánchez <ipadilla@neology.mx>, Bradley Feldmann <bfeldmann@neology.net>, John Tedona <jtedona@neology.net>, Luke Normington <LNormington@uk.neology.net>
Cc: ALPR_Support <ALPR_Support@neology.net>, Michael Roth <mroth@neology.net>, Enrique Martinez de Velasco <emartinez@neology.mx>, Victor Alan Miranda Cortez <vmiranda@neology.mx>, Michell Itallekzi Garcia Garcia <mgarcia@neology.mx>, Daniela Geraldine Ponce Calderon <dponce@neopartners.mx>, Giovanni Navarrete Araiza <gnavarrete@neology.mx>
Subject: Re: Boss4 Dashboard

Go ahead with it. Thank you.

Respectfully,

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

From: Israel Padilla Sánchez <ipadilla@neology.mx>
Sent: Wednesday, May 17, 2023 4:36:08 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Bradley Feldmann <bfeldmann@neology.net>; John Tedona <jtedona@neology.net>; Luke Normington <LNormington@uk.neology.net>
Cc: ALPR_Support <ALPR_Support@neology.net>; mroth <mroth@neology.net>; Enrique Martinez de Velasco <emartinez@neology.mx>; Victor Alan Miranda Cortez <vmiranda@neology.mx>; Michell Itallekzi Garcia Garcia <mgarcia@neology.mx>; Daniela Geraldine Ponce Calderon <dponce@neopartners.mx>; Giovanni Navarrete Araiza <gnavarrete@neology.mx>
Subject: Re: Boss4 Dashboard

CAUTION: This email originated from a sender outside of the 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, Sergeant,

Yes, if you agree, we will apply the update tonight.

There will be a brief interruption in the service around midnight.

Regards
--
Israel Padilla

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Sent: Wednesday, May 17, 2023 1:41 PM
To: Bradley Feldmann <bfeldmann@neology.net>; Israel Padilla Sánchez <ipadilla@neology.mx>; John Tedona <jtedona@neology.net>; Luke Normington <LNormington@uk.neology.net>
Cc: ALPR_Support <ALPR_Support@neology.net>; Michael Roth <mroth@neology.net>; Enrique Martinez de Velasco <emartinez@neology.mx>; Victor Alan Miranda Cortez <vmiranda@neology.mx>; Michell Itallekzi Garcia Garcia <mgarcia@neology.mx>; Daniela Geraldine Ponce Calderon <dponce@neopartners.mx>; Giovanni Navarrete Araiza <gnavarrete@neology.mx>
Subject: Re: Boss4 Dashboard

Israel,

With that bug resolved, are we prepared to do the software update?

Respectfully,

Noah

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

From: Bradley Feldmann <bfeldmann@neology.net>
Sent: Monday, May 15, 2023 7:29 AM
To: Israel Padilla Sánchez <ipadilla@neology.mx>; John Tedona <jtedona@neology.net>; Luke Normington <LNormington@uk.neology.net>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: ALPR_Support <ALPR_Support@neology.net>; mroth <mroth@neology.net>; Enrique Martinez de Velasco <emartinez@neology.mx>; Victor Alan Miranda Cortez <vmiranda@neology.mx>; Michell Itallekzi Garcia Garcia <mgarcia@neology.mx>; Daniela Geraldine Ponce Calderon <dponce@neopartners.mx>; Giovanni Navarrete Araiza <gnavarrete@neology.mx>
Subject: Re: Boss4 Dashboard

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

Israel: thanks very much

Noah: FYI

From: Israel Padilla Sánchez <ipadilla@neology.mx>
Date: Sunday, May 14, 2023 at 11:30 PM
To: John Tedona <jtedona@neology.net>, Bradley Feldmann <bfeldmann@neology.net>, Luke Normington <LNormington@uk.neology.net>
Cc: ALPR_Support <ALPR_Support@neology.net>, Michael Roth <mroth@neology.net>, Enrique Martinez de Velasco <emartinez@neology.mx>, Victor Alan Miranda Cortez <vmiranda@neology.mx>, Michell Itallekzi Garcia Garcia <mgarcia@neology.mx>, Daniela Geraldine Ponce Calderon <dponce@neopartners.mx>, Giovanni Navarrete Araiza <gnavarrete@neology.mx>
Subject: Re: Boss4 Dashboard

Hi all,

The recovery of the reads has been completed.

<image.png>

Regards

--
Israel Padilla

From: John Tedona <jtedona@neology.net>
Sent: Friday, May 12, 2023 11:46 AM
To: Israel Padilla Sánchez <ipadilla@neology.mx>; Bradley Feldmann <bfeldmann@neology.net>; Luke Normington <LNormington@uk.neology.net>
Cc: ALPR_Support <ALPR_Support@neology.net>; Michael Roth <mroth@neology.net>; Enrique Martinez de Velasco <emartinez@neology.mx>; Victor Alan Miranda Cortez <vmiranda@neology.mx>; Michell Itallekzi Garcia Garcia <mgarcia@neology.mx>; Daniela Geraldine Ponce Calderon <dponce@neopartners.mx>; Giovanni Navarrete Araiza <gnavarrete@neology.mx>
Subject: RE: Boss4 Dashboard

Israel, Thanks for update. Please let me know, or feel free to notify Noah directly when the recovery has been completed.

Thanks,

<image001.png>

John Tedona
Sales Manager

Mobile: 201-[redacted]
Email: jtedona@neology.net

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

www.neology.net

<image002.png>
<image003.png>

***Customer Support& Sales*:** (833) 747-7LPR or (833) 747-7577
Alpr_support@neology.net – Technical Service/Repair
Alpr@neology.net - Sales Inquiry
https://www.policegrantshelp.com/neology-grant-assistance/ - Grant Assistance

From: Israel Padilla Sánchez <ipadilla@neology.mx>
Sent: Friday, May 12, 2023 1:41 PM
To: Bradley Feldmann <bfeldmann@neology.net>; John Tedona <jtedona@neology.net>; Luke Normington <LNormington@uk.neology.net>
Cc: ALPR_Support <ALPR_Support@neology.net>; Michael Roth <mroth@neology.net>; Enrique Martinez de Velasco <emartinez@neology.mx>; Victor Alan Miranda Cortez <vmiranda@neology.mx>; Michell Itallekzi Garcia Garcia <mgarcia@neology.mx>; Daniela Geraldine Ponce Calderon <dponce@neopartners.mx>; Giovanni Navarrete Araiza <gnavarrete@neology.mx>
Subject: Re: Boss4 Dashboard

Hi all,

The hits' recovery was completed last night. There's no loss of any data. The reads recovery is ongoing, right now we have recovered until July 10th.

Regards
--
Israel Padilla

From: Bradley Feldmann <bfeldmann@neology.net>
Sent: Thursday, May 11, 2023 3:53 PM
To: Israel Padilla Sánchez <ipadilla@neology.mx>
Cc: John Tedona <jtedona@neology.net>; Luke Normington <LNormington@uk.neology.net>; ALPR_Support <ALPR_Support@neology.net>; Michael Roth <mroth@neology.net>; Enrique Martinez de Velasco <emartinez@neology.mx>; Victor Alan Miranda Cortez <vmiranda@neology.mx>; Michell Itallekzi Garcia Garcia <mgarcia@neology.mx>; Daniela Geraldine Ponce Calderon <dponce@neopartners.mx>; Giovanni Navarrete Araiza <gnavarrete@neology.mx>
Subject: Re: Boss4 Dashboard

Good by me
Thanks much

Sent from my iPhone

> On May 11, 2023, at 12:16 PM, Israel Padilla Sánchez <ipadilla@neology.mx> wrote:
>
> Hi all,
>
> Thank you for the meeting today morning. Here's a brief

summary of the events of this issue.

Last Tuesday it was found that the numbers of hits and reads were significantly lower than the previous week. It was confirmed in the purge metrics table that the retention microservice was deleting the data since last Saturday. As soon as this was detected, we stopped the retention microservice and started the recovery of the hits and reads.

Yesterday night, all the hits until May 6th (just before the purge started) are recovered successfully. The final portion of the hits will be recovered today. Regarding the reads, we are recovering them at this moment and we estimate 72-96 hours to fully recover them. There will be no loss of data. Right now the gap is from June 1st, 2022 until September 15th, 2022.

QA and Dev teams are testing the new retention microservice with the fix of this issue.

This is the technical summary of the issue:

Configuration:

a. Massachusetts Host has a staging site that is configured to preserve the reads from the cameras inside this agency for up to 2 days.
b. All the tenants, apart from the Host, are configured to keep the data of the cameras for up to 1 year.
c. All the operative cameras are placed in the tenant "Massachusetts State Police" (it has a retention policy of 1 year)

Steps that caused the issue

1. On May 6th after 15:00 hours, a new agency was created by a user in BOSS4.
2. The agency was created without retention policies, so it is supposed to take the retention policy configuration from the Regional Provider.
3. At 16:00 hours, the purge process was started automatically by the retention microservice.
    a. Due to a bug in the retention microservice, the retention policy of the Host (2 days) was used to purge data on all devices of the system.
4. The first kind of data that was deleted was the hits. Then the reads. The rate to delete reads was 1.5M per hour.
5. The reads deleted from the DB are recoverable using the Point In Time Restore of MongoDB. The Images are recoverable with the versioning of AWS S3.

Any questions, please let me know.

Regards
--
Israel Padilla

From: John Tedona <jtedona@neology.net>
Sent: Wednesday, May 10, 2023 7:24 PM
To: Giovanni Navarrete Araiza <gnavarrete@neology.mx>; Luke Normington <LNormington@uk.neology.net>; Bradley Feldmann <bfeldmann@neology.net>
Cc: Israel Padilla Sánchez <ipadilla@neology.mx>; ALPR_Support <ALPR_Support@neology.net>; Michael Roth <mroth@neology.net>; Enrique Martinez de Velasco <emartinez@neology.mx>; Victor Alan Miranda Cortez <vmiranda@neology.mx>; Michell Itallekzi Garcia Garcia <mgarcia@neology.mx>; Daniela Geraldine Ponce Calderon <dponce@neopartners.mx>
Subject: RE: Boss4 Dashboard

Giovanni and team,

There's always a silver lining. I'm glad to hear that the data was retained. I look forward to tomorrow's discussion to draft our response.

John Tedona
Sales Manager

Mobile: 201-[redacted]
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
https://www.policegrantshelp.com/neology-grant-assistance/ - Grant Assistance

From: Giovanni Navarrete Araiza <gnavarrete@neology.mx>
Sent: Wednesday, May 10, 2023 7:31 PM
To: Luke Normington <LNormington@uk.neology.net>; John Tedona <jtedona@neology.net>; Bradley Feldmann <bfeldmann@neology.net>
Cc: Israel Padilla Sánchez <ipadilla@neology.mx>; ALPR_Support <ALPR_Support@neology.net>; Michael Roth <mroth@neology.net>; Enrique Martinez de Velasco <emartinez@neology.mx>; Victor Alan Miranda Cortez <vmiranda@neology.mx>; Michell Itallekzi Garcia Garcia <mgarcia@neology.mx>; Daniela Geraldine Ponce Calderon <dponce@neopartners.mx>
Subject: Re: Boss4 Dashboard

Hi all,

After further analysis in the morning, the team detected an abnormal situation that led to the deletion of reads and hits due to incorrect application of the retention policy.

It's a misapplied trading rule situation, similar to the one Noah mentions, which occurred in September of last year, but not exactly the same.

At this moment he is already in the process of recovering the information, first Hits and then the readings.

No loss of information is expected at all.

Israel will send a more complete report so that John can tell us what is the best way to communicate it to Noah.

Giovanni Navarrete

Enviado desde mi iPhone

> El 10 may 2023, a la(s) 16:04, Luke Normington <LNormington@uk.neology.net> escribió:
>
> Israel
>
> Keen to hear your technical input on this. Was it a User Interface issue? Or something else? Various reasons why spike in hits could be observed (genuine reasons, as well as spurious reasons).
>
> Can you please provide internal assessment prior to sharing

with Noah. For example, you mentioned the retention microservice in your mail below - was the working theory yesterday that on 80k reads on the counter a consequence of retention microservice not correctly cleansing/cleaning out the hits because of an issue with retention microservice.

@John Tedona - can you relay to the team what you said to Noah, aside from setting up a meeting? Was it a long discussion?

Thanks
Luke

Thanks
Luke

Luke Normington

Managing Director

Phone: + 44 (0)1256 581134

Mobile: + 44 (0)7375 024539

Email: lnormington@uk.neology.net

Unit 2 Moorside Place, Moorside Road,
Winchester, SO23 7FX

www.neology.net

Registered Office: 6th Floor, Kildare House, Dorset Rise, London, United Kingdom, EC4Y 8EN Registered in England & Wales, No 10809863.

The information contained in this communication is confidential and intended only for the use of the recipient named and may also be legally privileged. If you are not

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

From: John Tedona <jtedona@neology.net>
Sent: Wednesday, 10 May 2023, 22:51
To: Israel Padilla Sánchez <ipadilla@neology.mx>; Bradley Feldmann <bfeldmann@neology.net>
Cc: ALPR Support <ALPR_Support@neology.net>; Michael Roth <mroth@neology.net>; Giovanni Navarrete Araiza <gnavarrete@neology.mx>; Enrique Martinez de Velasco <emartinez@neology.mx>; Victor Alan Miranda Cortez <vmiranda@neology.mx>; Michell Itallekzi Garcia Garcia <mgarcia@neology.mx>; Daniela Geraldine Ponce Calderon <dponce@neopartners.mx>; Luke Normington <LNormington@uk.neology.net>
Subject: RE: Boss4 Dashboard

Israel et al.

Noah's brief email from yesterday belies his frustration….he waits to vent his true frustration when he calls me. For some background: He had to respond to an OPRA (open public records request) for ALPR information last week. He recalled that there were around 27M reads and 80K hits at the time last week; however yesterday he noted that read and hit data was missing since he saw that there was only 27M reads and 60K hits on the dash board (I forget the exact numbers). He reminded me that this same issue happened 2 or 3 months ago and that we gave him assurance it wouldn't happen again.

This type of missing data has the potential to be non-recoverable in maintaining this account. For example if

he has to respond to a second OPRA and the data set is different than the data set from the previous request, MSP's ALPR data will be viewed as questionable and rendered as unusable in court. Hopefully as before this data can be recovered. Noah made it very clear to me that If we ever actually lose data it would cause MSP to dismantle their ALPR program.

Noah asked that we hold another status meeting next week. The invite to follow shortly.

Please put in place whatever checks and balances are necessary to prevent this from reoccurring.

Thanks

John Tedona
Sales Manager

Mobile: 201-[redacted]
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
https://www.policegrantshelp.com/neology-grant-assistance/ - Grant Assistance

---

From: Israel Padilla Sánchez <ipadilla@neology.mx>
Sent: Wednesday, May 10, 2023 12:26 AM
To: Bradley Feldmann <bfeldmann@neology.net>
Cc: Pack, Noah (POL) <noah.pack@state.ma.us>; ALPR_Support <ALPR_Support@neology.net>; Michael Roth <mroth@neology.net>; Giovanni Navarrete Araiza <gnavarrete@neology.mx>; Enrique Martinez de Velasco

<emartinez@neology.mx>; John Tedona <jtedona@neology.net>; Victor Alan Miranda Cortez <vmiranda@neology.mx>; Michell Itallekzi Garcia Garcia <mgarcia@neology.mx>; Daniela Geraldine Ponce Calderon <dponce@neopartners.mx>
Subject: Re: Boss4 Dashboard

Hi Sergeant,

I have done a modification over the hits graph. The issue was a point that had a very high number of hits. We are still investigating why this spike happened.

Also, we are working on rebuilding the hits counter. It is related to the retention microservice. We will let you know more detail about this tomorrow.

Due to this, I'm deferring the update of the application.

Best regards
--
Israel Padilla

From: Israel Padilla Sánchez
Sent: Tuesday, May 9, 2023 7:10 PM
To: Bradley Feldmann <bfeldmann@neology.net>
Cc: Pack, Noah (POL) <noah.pack@state.ma.us>; ALPR Support <ALPR_Support@neology.net>; Michael Roth <mroth@neology.net>; Giovanni Navarrete Araiza <gnavarrete@neology.mx>; Enrique Martinez de Velasco <emartinez@neology.mx>; John Tedona <jtedona@neology.net>; Victor Alan Miranda Cortez <vmiranda@neology.mx>; Michell Itallekzi Garcia Garcia <mgarcia@neology.mx>; Daniela Geraldine Ponce Calderon <dponce@neopartners.mx>
Subject: Re: Boss4 Dashboard

It seems like the hits on the system decreased significantly.

I'll need to review the DB to confirm the numbers.

I'm on my way home, as soon as I get there I'll let you know

what I find

Regards
Israel

Sent from my iPhone

> On 9 May 2023, at 19:01, Bradley Feldmann <bfeldmann@neology.net> wrote:
>
> Giovanni / Israel: please advise
>
> ---
>
> **From:** Pack, Noah (POL) <noah.pack@state.ma.us>
> **Date:** Tuesday, May 9, 2023 at 7:58 PM
> **To:** ALPR_Support <ALPR_Support@neology.net>, Israel Padilla Sánchez <ipadilla@neology.mx>, Michael Roth <mroth@neology.net>, Bradley Feldmann <bfeldmann@neology.net>
> **Cc:** John Tedona <jtedona@neology.net>
> **Subject:** Boss4 Dashboard
>
> Israel,
>
> Please check the reads/hits displayed on the dashboard in Boss4 and advise on the database status.
>
> Respectfully,
>
> **Sergeant Noah H. Pack**
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> Office of the Division Commander

From: Brian Gilkey
To: Cyr, Mark (POL)
Subject: Re: Catching-up
Date: Friday, August 4, 2023 2:45:59 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.

Hey Mark -

Looks like 24th & 25th are gonna be the dates. How does coffee on the 25th work? The afternoon of the 24th works as well, so just let me know what's easiest for you. We can meet at or near HQ or whatever is convenient. I'm thinking I might stay downtown since I've gotta hit BC, BU, Northeastern.

Enjoy your vacation!

Brian

On Tue, 1 Aug 2023 at 09:53, Cyr, Mark (POL) <mark.cyr@pol.state.ma.us> wrote:

> Very interesting polls. Thank you. Access to ALPR data topped the list of wanted sources... not surprising. ALPR has become an extremely valuable investigative tool.
>
> *Lieutenant Colonel Mark D. Cyr #2728*
> *Massachusetts State Police*
> *Division Commander*
> *Division of Homeland Security and Preparedness*
> *508-988-7301 (office)*
> [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:** Brian Gilkey <brian.gilkey@siren.io>
> **Sent:** Tuesday, August 1, 2023 9:18 AM
> **To:** Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
> **Subject:** Re: Catching-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.
>
> Hey Mark -
>
> Thanks for the note. Good news on the projects coming to completion! We've actually done quite a bit to the Siren Platform since the last time you saw it. In fact, we've kinda revamped the LE offering, but I can catch you up when we meet up.

From: Brian Gilkey
To: Cyr, Mark (POL)
Subject: Re: Catching-up
Date: Tuesday, August 1, 2023 10:43:45 AM

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

Piece of cake.

On Tue, 1 Aug 2023 at 09:53, Cyr, Mark (POL) <mark.cyr@pol.state.ma.us> wrote:

> Very interesting polls. Thank you. Access to ALPR data topped the list of wanted sources... not surprising. ALPR has become an extremely valuable investigative tool.
>
> *Lieutenant Colonel Mark D. Cyr #2728*
> *Massachusetts State Police*
> *Division Commander*
> *Division of Homeland Security and Preparedness*
> *508-988-7301 (office)*
> [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:** Brian Gilkey <brian.gilkey@siren.io>
> **Sent:** Tuesday, August 1, 2023 9:18 AM
> **To:** Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
> **Subject:** Re: Catching-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.
>
> Hey Mark -
>
> Thanks for the note. Good news on the projects coming to completion! We've actually done quite a bit to the Siren Platform since the last time you saw it. In fact, we've kinda revamped the LE offering, but I can catch you up when we meet up.
>
> I'll definitely keep you posted on my plans, but we were looking at either 8/17-8/18 or the following week 8/24-8/25. As soon as I zero in, I'll shoot you a text.
>
> Lastly, just in case you need some reading material (haha), I've attached a recent graphic as well as results from a flash poll we conducted and published with The Government Business Council.
>
> Brian

On Fri, 28 Jul 2023 at 10:00, Cyr, Mark (POL) <mark.cyr@pol.state.ma.us> wrote:

Good morning Brian,
Here at DHS, things are busy as usual, and we have several exciting projects that are nearing completion. Things have been moving very slowly with the Colonel search, which is great for myself and the Department. Colonel Jack Mawn has been doing an exceptional job. G.L. c. 4. sec. 7.cl. 26 (c)(privacy) [redacted]

Keep me updated on your plans. I will be away from August 6th through August 13th. Would be great to catch up for a coffee.

I am planning to attend the IACP. Will be flying out on 10/13 and returning 10/17.

Mark

Lieutenant Colonel Mark D. Cyr #2728
Massachusetts State Police
Division Commander
Division of Homeland Security and Preparedness
508-988-7301 (office)
G.L. c. 4.sec. 7.cl.26 (n)(security) [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: Brian Gilkey <brian.gilkey@siren.io>
Sent: Thursday, July 27, 2023 3:01 PM
To: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Subject: Catching-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.

Hey there Mark -

I was trading texts with Dermot the other day on the Orioles and it reminded me we hadn't touched base in a while. Hopefully the dust has settled a little from the Colonel's retirement. How is the search for a new Colonel going? I hope you're still in the running.

I was actually looking at the calendar and trying to get up your way in the next couple of

weeks. My daughter is interested in a couple schools up that way and I thought I'd try and catch dinner with Dermot one night. Heck, I'd love to catch up with Chris as well. I was thinking we could grab a coffee and you could give me the low down on things.

Also, are you planning on going to IACP this year? If so, we can talk about that as well.

Cheers,

Brian

--

Brian K. Gilkey
Sales Director, Siren

1735 Market Street, Suite A498, Philadelphia, PA 19103, USA
410-336-0608 brian.gilkey@siren.io www.siren.io

--

Brian K. Gilkey
Sales Director, Siren

1735 Market Street, Suite A498, Philadelphia, PA 19103, USA
410-336-0608 brian.gilkey@siren.io www.siren.io

--

Brian K. Gilkey
Sales Director, Siren

1735 Market Street, Suite A498, Philadelphia, PA 19103, USA
410-336-0608 brian.gilkey@siren.io www.siren.io

From: Cyr, Mark (POL)
To: Brian Gilkey
Subject: Re: Catching-up
Date: Tuesday, August 1, 2023 9:53:42 AM

Very interesting polls. Thank you. Access to ALPR data topped the list of wanted sources... not surprising. ALPR has become an extremely valuable investigative tool.

Lieutenant Colonel Mark D. Cyr #2728
Massachusetts State Police
Division Commander
Division of Homeland Security and Preparedness
508-988-7301 (office)
[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: Brian Gilkey <brian.gilkey@siren.io>
Sent: Tuesday, August 1, 2023 9:18 AM
To: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Subject: Re: Catching-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.

Hey Mark -

Thanks for the note. Good news on the projects coming to completion! We've actually done quite a bit to the Siren Platform since the last time you saw it. In fact, we've kinda revamped the LE offering, but I can catch you up when we meet up.

I'll definitely keep you posted on my plans, but we were looking at either 8/17-8/18 or the following week 8/24-8/25. As soon as I zero in, I'll shoot you a text.

Lastly, just in case you need some reading material (haha), I've attached a recent graphic as well as results from a flash poll we conducted and published with The Government Business Council.

Brian

On Fri, 28 Jul 2023 at 10:00, Cyr, Mark (POL) <mark.cyr@pol.state.ma.us> wrote:

> Good morning Brian,
> Here at DHS, things are busy as usual, and we have several exciting projects that are nearing completion. Things have been moving very slowly with the Colonel search, which is great

for myself and the Department. Colonel Jack Mawn has been doing an exceptional job. [redacted]

Keep me updated on your plans. I will be away from August 6th through August 13th. Would be great to catch up for a coffee.

I am planning to attend the IACP. Will be flying out on 10/13 and returning 10/17.

Mark

Lieutenant Colonel Mark D. Cyr #2728
Massachusetts State Police
Division Commander
Division of Homeland Security and Preparedness
508-988-7301 (office)
[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: Brian Gilkey <brian.gilkey@siren.io>
Sent: Thursday, July 27, 2023 3:01 PM
To: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Subject: Catching-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.

Hey there Mark -

I was trading texts with Dermot the other day on the Orioles and it reminded me we hadn't touched base in a while. Hopefully the dust has settled a little from the Colonel's retirement. How is the search for a new Colonel going? I hope you're still in the running.

I was actually looking at the calendar and trying to get up your way in the next couple of weeks. My daughter is interested in a couple schools up that way and I thought I'd try and catch dinner with Dermot one night. Heck, I'd love to catch up with Chris as well. I was thinking we could grab a coffee and you could give me the low down on things.

Also, are you planning on going to IACP this year? If so, we can talk about that as well.

Cheers,

Brian

--

Brian K. Gilkey
Sales Director, Siren

1735 Market Street, Suite A498, Philadelphia, PA 19103, USA
410-336-0608 brian.gilkey@siren.io www.siren.io

--

Brian K. Gilkey
Sales Director, Siren

1735 Market Street, Suite A498, Philadelphia, PA 19103, USA
410-336-0608 brian.gilkey@siren.io www.siren.io

From: Cyr, Mark (POL)
To: Brian Gilkey
Subject: Re: Catching-up
Date: Sunday, August 6, 2023 8:23:57 AM

The morning of the 25th sounds great. Lets plan to touch base a few days before to iron out the details.

Mark

Lieutenant Colonel Mark D. Cyr #2728
Massachusetts State Police
Division Commander
Division of Homeland Security and Preparedness
508-988-7301 (office)
G.L. c. 4,sec. 7,cl.26 (n)(security) *(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: Brian Gilkey <brian.gilkey@siren.io>
Sent: Friday, August 4, 2023 2:45 PM
To: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Subject: Re: Catching-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.

Hey Mark -

Looks like 24th & 25th are gonna be the dates. How does coffee on the 25th work? The afternoon of the 24th works as well, so just let me know what's easiest for you. We can meet at or near HQ or whatever is convenient. I'm thinking I might stay downtown since I've gotta hit BC, BU, Northeastern.

Enjoy your vacation!

Brian

On Tue, 1 Aug 2023 at 09:53, Cyr, Mark (POL) <mark.cyr@pol.state.ma.us> wrote:

> Very interesting polls. Thank you. Access to ALPR data topped the list of wanted sources... not surprising. ALPR has become an extremely valuable investigative tool.
>
> *Lieutenant Colonel Mark D. Cyr #2728*
> *Massachusetts State Police*

Division Commander
Division of Homeland Security and Preparedness
508-988-7301 (office)
G.L. c. 4 sec. 7.cl 26 (m)(security) *(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: Brian Gilkey <brian.gilkey@siren.io>
Sent: Tuesday, August 1, 2023 9:18 AM
To: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Subject: Re: Catching-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.

Hey Mark -

Thanks for the note. Good news on the projects coming to completion! We've actually done quite a bit to the Siren Platform since the last time you saw it. In fact, we've kinda revamped the LE offering, but I can catch you up when we meet up.

I'll definitely keep you posted on my plans, but we were looking at either 8/17-8/18 or the following week 8/24-8/25. As soon as I zero in, I'll shoot you a text.

Lastly, just in case you need some reading material (haha), I've attached a recent graphic as well as results from a flash poll we conducted and published with The Government Business Council.

Brian

On Fri, 28 Jul 2023 at 10:00, Cyr, Mark (POL) <mark.cyr@pol.state.ma.us> wrote:

> Good morning Brian,
> Here at DHS, things are busy as usual, and we have several exciting projects that are nearing completion. Things have been moving very slowly with the Colonel search, which is great for myself and the Department. Colonel Jack Mawn has been doing an exceptional job. G.L. c. 4. sec. 7.cl. 26 (c)(privacy)
>
> Keep me updated on your plans. I will be away from August 6th through August 13th. Would be great to catch up for a coffee.
>
> I am planning to attend the IACP. Will be flying out on 10/13 and returning 10/17.

Mark

Lieutenant Colonel Mark D. Cyr #2728
Massachusetts State Police
Division Commander
Division of Homeland Security and Preparedness
508-988-7301 (office)
[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: Brian Gilkey <brian.gilkey@siren.io>
Sent: Thursday, July 27, 2023 3:01 PM
To: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Subject: Catching-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.

Hey there Mark -

I was trading texts with Dermot the other day on the Orioles and it reminded me we hadn't touched base in a while. Hopefully the dust has settled a little from the Colonel's retirement. How is the search for a new Colonel going? I hope you're still in the running.

I was actually looking at the calendar and trying to get up your way in the next couple of weeks. My daughter is interested in a couple schools up that way and I thought I'd try and catch dinner with Dermot one night. Heck, I'd love to catch up with Chris as well. I was thinking we could grab a coffee and you could give me the low down on things.

Also, are you planning on going to IACP this year? If so, we can talk about that as well.

Cheers,

Brian

--

Brian K. Gilkey
Sales Director, Siren

1735 Market Street, Suite A498, Philadelphia, PA 19103, USA
410-336-0608 brian.gilkey@siren.io www.siren.io

--

Brian K. Gilkey
Sales Director, Siren

1735 Market Street, Suite A498, Philadelphia, PA 19103, USA
410-336-0608 brian.gilkey@siren.io www.siren.io

--

Brian K. Gilkey
Sales Director, Siren

1735 Market Street, Suite A498, Philadelphia, PA 19103, USA
410-336-0608 brian.gilkey@siren.io www.siren.io

From: Farley, Michael (POL)
To: Sullivan, John (POL)
Cc: Banik, John (POL); Keefe, Joseph (POL)
Subject: Re: FLock APLR
Date: Wednesday, August 2, 2023 5:57:51 PM

Sully-Write a To-From through channels and include LTC Cyr with a request to utilIze Flock for VFAS members and that is a proven, successful tool in fugitive invests. Also write that per policy, VFAS is called for Amber Alert activations and other exigency type matters. Thx

Get Outlook for iOS

From: Sullivan, John (POL) <john.sullivan@pol.state.ma.us>
Sent: Wednesday, August 2, 2023 1:46:39 PM
To: Farley, Michael (POL) <michael.farley@pol.state.ma.us>
Cc: Banik, John (POL) <John.Banik@pol.state.ma.us>; Keefe, Joseph (POL) <joseph.keefe@pol.state.ma.us>
Subject: FLock APLR

Major,

With the recent issues involving Callyo products, VFAS members want to make sure that it's acceptable to utilize Flock. After a little research (I had limited knowledge of it because, personally, I never used it). My understanding is "Flock Safety" is the name of the company. It's an American Company that basically sells ALPR technology to law enforcement agencies and neighborhood associations. Flock's cameras read license plates and send instant alerts to law enforcement officers based on a populated list. (Stolen cars, vehicles of interest). Unlike many other ALPR Systems, Flock camera's allow searches based on the car's color and various other visual features. TFR-11 addresses **"Use of Non-Departmental ALPR Systems"** of page 5 (of 8)**.**
The policy allows MSP members to contact other agencies to request assistance with information. Additionally, the policy states that that Supervisors and analysts from Watch Center & ALPR Admin. can access non departmental systems. However, the policy specifically states that other members shall not obtain/utilize accounts with permission for Lt. Col. Cyr.

Currently, multiple members (VFAS Metro & North) have Flock Accounts that they are utilizing for fugitive investigations. Revere PD has set up accounts for the Metro Guys and I believe Lynn gave Scali one or he retained his when he left Lynn. Each account has a unique sign in to access the data in and leaves a footprint. Currently, the Flock Map lists Quincy, Lynn, Revere, Winthrop, Everett & Malden as participating. Each local police department has an administrator for flock & that Admin. can asked permission (vIa email) to view each other's FLock Cameras. As recent as last Sunday (July 30, 2023), Tpr. Diliegro was able to utilize the Winthrop Flock Camera to catch a Revere Stabbing Suspect that had just returned home after being on the run and was wanted.

VFAS is utilizing Flock Safety cameras to apprehend wanted fugitives. Members of VFAS are not using it to develop PC or in the furtherance of an ongoing investigation/case. I have included Sgt. Joe Keefe on this email because he is well versed in the Flock Camera specifics. Thanks,

Sully

Detective Lieutenant John B. Sullivan #3359
Massachusetts State Police
Unit Commanderf
Violent Fugitive Apprehension Section
Office: 508-820-2374
Cell: [redacted]

From: Sullivan, John (POL)
To: Farley, Michael (POL)
Cc: Banik, John (POL); Keefe, Joseph (POL)
Subject: Re: FLock APLR
Date: Wednesday, August 2, 2023 2:33:31 PM

That's the German pronunciation.

Get Outlook for iOS

From: Farley, Michael (POL) <michael.farley@pol.state.ma.us>
Sent: Wednesday, August 2, 2023 2:30:57 PM
To: Sullivan, John (POL) <john.sullivan@pol.state.ma.us>
Cc: Banik, John (POL) <John.Banik@pol.state.ma.us>; Keefe, Joseph (POL) <joseph.keefe@pol.state.ma.us>
Subject: RE: FLock APLR

I'll have to review the policy and let you know. FYI-your title is listed as Unit Commanderf in your email signature

---

From: Sullivan, John (POL) <john.sullivan@pol.state.ma.us>
Sent: Wednesday, August 2, 2023 1:47 PM
To: Farley, Michael (POL) <michael.farley@pol.state.ma.us>
Cc: Banik, John (POL) <John.Banik@pol.state.ma.us>; Keefe, Joseph (POL) <joseph.keefe@pol.state.ma.us>
Subject: FLock APLR

Major,

With the recent issues involving Callyo products, VFAS members want to make sure that it's acceptable to utilize Flock. After a little research (I had limited knowledge of it because, personally, I never used it). My understanding is "Flock Safety" is the name of the company. It's an American Company that basically sells ALPR technology to law enforcement agencies and neighborhood associations. Flock's cameras read license plates and send instant alerts to law enforcement officers based on a populated list. (Stolen cars, vehicles of interest). Unlike many other ALPR Systems, Flock camera's allow searches based on the car's color and various other visual features. TFR-11 addresses **"Use of Non-Departmental ALPR Systems"** of page 5 (of 8)**.**
The policy allows MSP members to contact other agencies to request assistance with information. Additionally, the policy states that that Supervisors and analysts from Watch Center & ALPR Admin. can access non departmental systems. However, the policy specifically states that other members shall not obtain/utilize accounts with permission for Lt. Col. Cyr.

Currently, multiple members (VFAS Metro & North) have Flock Accounts that they are utilizing for fugitive investigations. Revere PD has set up accounts for the Metro Guys and I believe Lynn gave Scali one or he retained his when he left Lynn. Each account has a unique sign in to access the data in and leaves a footprint. Currently, the Flock Map lists Quincy, Lynn, Revere, Winthrop, Everett &

Malden as participating. Each local police department has an administrator for flock & that Admin. can asked permission (vIa email) to view each other's FLock Cameras. As recent as last Sunday (July 30, 2023), Tpr. Diliegro was able to utilize the Winthrop Flock Camera to catch a Revere Stabbing Suspect that had just returned home after being on the run and was wanted.

VFAS is utilizing Flock Safety cameras to apprehend wanted fugitives. Members of VFAS are not using it to develop PC or in the furtherance of an ongoing investigation/case. I have included Sgt. Joe Keefe on this email because he is well versed in the Flock Camera specifics. Thanks,

Sully

Detective Lieutenant John B. Sullivan #3359
Massachusetts State Police

Unit Commanderf

Violent Fugitive Apprehension Section

Office: 508-820-2374

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

From: Sullivan, John (POL)
To: Farley, Michael (POL)
Cc: Banik, John (POL); Keefe, Joseph (POL)
Subject: Re: FLock APLR
Date: Wednesday, August 2, 2023 6:35:34 PM

Okay. Will do & thanks

Get Outlook for iOS

From: Farley, Michael (POL) <michael.farley@pol.state.ma.us>
Sent: Wednesday, August 2, 2023 5:57:50 PM
To: Sullivan, John (POL) <john.sullivan@pol.state.ma.us>
Cc: Banik, John (POL) <John.Banik@pol.state.ma.us>; Keefe, Joseph (POL) <joseph.keefe@pol.state.ma.us>
Subject: Re: FLock APLR

Sully-Write a To-From through channels and include LTC Cyr with a request to utilIze Flock for VFAS members and that is a proven, successful tool in fugitive invests. Also write that per policy, VFAS is called for Amber Alert activations and other exigency type matters. Thx

Get Outlook for iOS

From: Sullivan, John (POL) <john.sullivan@pol.state.ma.us>
Sent: Wednesday, August 2, 2023 1:46:39 PM
To: Farley, Michael (POL) <michael.farley@pol.state.ma.us>
Cc: Banik, John (POL) <John.Banik@pol.state.ma.us>; Keefe, Joseph (POL) <joseph.keefe@pol.state.ma.us>
Subject: FLock APLR

Major,

With the recent issues involving Callyo products, VFAS members want to make sure that it's acceptable to utilize Flock. After a little research (I had limited knowledge of it because, personally, I never used it). My understanding is "Flock Safety" is the name of the company. It's an American Company that basically sells ALPR technology to law enforcement agencies and neighborhood associations. Flock's cameras read license plates and send instant alerts to law enforcement officers based on a populated list. (Stolen cars, vehicles of interest). Unlike many other ALPR Systems, Flock camera's allow searches based on the car's color and various other visual features. TFR-11 addresses **"Use of Non-Departmental ALPR Systems"** of page 5 (of 8)**.**
The policy allows MSP members to contact other agencies to request assistance with information. Additionally, the policy states that that Supervisors and analysts from Watch Center & ALPR Admin. can access non departmental systems. However, the policy specifically states that other members shall not obtain/utilize accounts with permission for Lt. Col. Cyr.

Currently, multiple members (VFAS Metro & North) have Flock Accounts that they are utilizing for fugitive investigations. Revere PD has set up accounts for the Metro Guys and I believe Lynn gave Scali one

or he retained his when he left Lynn. Each account has a unique sign in to access the data in and leaves a footprint. Currently, the Flock Map lists Quincy, Lynn, Revere, Winthrop, Everett & Malden as participating. Each local police department has an administrator for flock & that Admin. can asked permission (vIa email) to view each other's FLock Cameras. As recent as last Sunday (July 30, 2023), Tpr. Diliegro was able to utilize the Winthrop Flock Camera to catch a Revere Stabbing Suspect that had just returned home after being on the run and was wanted.

VFAS is utilizing Flock Safety cameras to apprehend wanted fugitives. Members of VFAS are not using it to develop PC or in the furtherance of an ongoing investigation/case. I have included Sgt. Joe Keefe on this email because he is well versed in the Flock Camera specifics. Thanks,

Sully

Detective Lieutenant John B. Sullivan #3359
Massachusetts State Police
Unit Commanderf
Violent Fugitive Apprehension Section
Office: 508-820-2374
Cell: [redacted]

From: Pack, Noah (POL)
To: Jeremy Workman
Subject: Re: Hotlist Notification Setup
Date: Monday, July 3, 2023 12:57:34 PM

Hi Jeremy,

Thanks for the response and the feedback.

It is advisable and CJIS best practices to have an associated account for each individual recipient for emails.

Having fewer user accounts is arguably a CJIS better practice, as setting up a number of ghost accounts just to enable an email gateway inflates user account numbers, administrative workload, and creates an increased number of avenues for improper system access or compromise, since these accounts are left active but will never be set up or logged into. Most users need to receive alerts for specific data of relevance to them, not to log in and access the system.

We offer an external email alert on a per Hot-Plate option, but is not provided for Automated large lists.

This is valuable on the hot-plate feature and will suffice for most of our day to day requests, but it is a functional gap that it cannot be used at the hot list level. It is a gap that does not exist in our current system, which means I have to identify a workable solution and make it available to our system users. There are a number of use cases for this beyond the first one mentioned, such as notifying patrol users of stolen vehicles in their area (installing and configuring TAS software on all of their computers is again wildly more cumbersome than enabling the LPR system to simply send them an email).

If you are looking for a workaround, the recommended solution is to have your IT setup an email distribution list of users to receive these alerts. Then we can configure a single User to configure the alerting options on a specific Alert type across a larger list.

This would be a good work around for a static user list. However this user list changes by incident and occasion and would not be under our LPR system administrators' control to update. It is not feasible to create multiple email distribution lists that are routinely changed or updated but that we can't control.

Jeremy, would you be willing to set up a call after the 4th to go over general updates and a few of the LEARN features like these that we are trying to navigate? This interface feels clunky and complicated, as we've mentioned before, and the mental gymnastics we've got to do to make it work is problematic. I know updates are in the works, but we are trying to migrate away from another vendor for issues like this, and I'm already getting push back from our small number of LEARN users that things are more difficult for them, not less. I've got to make this work, as this program is too important to fail. Your help would be

immeasurably valuable to this process.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Investigative Services
Critical Incident Technical Investigations (CITI)
G.L. c. 4.sec. 7.cl.26 (n)(security)

From: Jeremy Workman <jeremy.workman@motorolasolutions.com>
Sent: Monday, July 3, 2023 12:09 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Daniel Wilburn <daniel.wilburn@motorolasolutions.com>; Sean Derbyshire <sean.derbyshire@motorolasolutions.com>
Subject: Re: Hotlist Notification Setup

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

Hello Noah,

It is advisable and CJIS best practices to have an associated account for each individual recipient for emails. We offer an external email alert on a per Hot-Plate option, but is not provided for Automated large lists.

If you are looking for a workaround, the recommended solution is to have your IT setup an email distribution list of users to receive these alerts. Then we can configure a single User to configure the alerting options on a specific Alert type across a larger list.

Example:

Create a list of users with your IT under single Email distribution list: MSI.ALPR.TerroristWatchlist@state.ma.us

Within LEARN, create an account with the Distro Email and assign desired Hotlist on load (or all agency users) and configure the "Alert Management" section to receive the desired alert/s and desired locations.

Regards,

On Mon, Jul 3, 2023 at 11:56 AM Pack, Noah (POL) <noah.pack@state.ma.us> wrote:

> Hey guys,
>
> I just spoke to support again about setting up hotlist notifications for another use case and

was met with another sorry we can't do that. I'm starting to get concerned by the limitations of the notification features in LEARN.

Could we set up a call in the near future to discuss some of the notification use cases here to see if we can work around or close these gaps? Thanks again for your time.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Investigative Services
Critical Incident Technical Investigations (CITI)

From: Pack, Noah (POL)
Sent: Monday, July 3, 2023 11:15 AM
To: Daniel Wilburn <daniel.wilburn@motorolasolutions.com>; Jeremy Workman <jeremy.workman@motorolasolutions.com>
Cc: Sean Derbyshire <sean.derbyshire@motorolasolutions.com>
Subject: Hotlist Notification Setup

Another troubleshooting question for you guys:

We are looking to setup notifications to a group of email addresses to receive alerts from a specific category of hits from a specific device (and eventually set of devices). This is a common workflow for us across a variety of use cases, but it happens to be relevant now due to July 4th security operations.

Here's an example:

Goal: generate alerts to go out to email address of users without LEARN accounts
Alert type: one sub-category (i.e. terrorist watch list plates) from the automatically updated MA-NCIC hotlist file
Device restrictions: devices located in a certain region only; this is currently done by selecting specific devices but could also be done with a geo zone.

I called technical support to discuss this prior to reaching out to you guys, and they indicated they are unaware of how this can be done without setting up and configuring LEARN accounts and notification settings for all the recipients, which isn't a viable option for us, due at least in part to the complexity of setting up and configuring LEARN accounts and the

associated alerts.

Thank you for allowing me to contact you guys directly, as you are exceptional problem solvers with this stuff, and I appreciate your help as we work to transition into making Vigilant work for MSP.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Investigative Services
Critical Incident Technical Investigations (CITI)

--

Jeremy Workman
Senior Product Manager, Vigilant
Mobile Video & Analytics **m:** +1 [redacted: G.L. c. 4,sec. 7,cl.26 (n)(security), G.L. c. 4]

This email and any attachments are for the authorized recipient's use only. If you receive this email in error, please immediately delete it from your system and notify the sender. You must not disclose, print, re-transmit, store, copy or rely on any part of this email and any attachments if you are not the authorized recipient. This email and any attachments are confidential and may contain confidential information and/or copyright material of Motorola Solutions, Inc.

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

From: Jeremy Workman
To: Pack, Noah (POL)
Subject: Re: Hotlist Notification Setup
Date: Monday, July 3, 2023 1:56:34 PM

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

Hello Noah,

We can discuss some of the hurdles for alerting external non-users. When we assign Hot-Lists, we assign to Users, User Groups, or Agency Wide. Thus, when we set up single external Hot-Plate alerts, it is going to alert on all alerts by that vehicle and not limited to zone or location. The recommended solution of loading all users resolves this by allowing us to assign groups or specific Hot Lists to the set of users.

Here is an idea to float you, we can set up a series of users via Bulk-load that can have no LEARN-Permissions, other than to be assigned a Hotlist and get an Email alert on them. This essentially would be tantamount to just an Email list that is ported to LEARN in the form of user accounts with no permissions. They also can be configured to login and only see the "My Profile" icon to configure their desired alerts. This would allow LPR System Administrators to have ultimate control of adding, removing, and assigning desired alerts on a per-email address. The users can be bulk-loaded via a template under the bulk load option within User Management.

I set up a call to discuss Email alerting options next week and any other items we would need to navigate to see the success of this program for Massachusetts State Police.

Regards,

On Mon, Jul 3, 2023 at 12:57 PM Pack, Noah (POL) <noah.pack@state.ma.us> wrote:

> Hi Jeremy,
>
> Thanks for the response and the feedback.
>
> It is advisable and CJIS best practices to have an associated account for each individual recipient for emails.
>
> *Having fewer user accounts is arguably a CJIS better practice, as setting up a number of ghost accounts just to enable an email gateway inflates user account numbers, administrative workload, and creates an increased number of avenues for improper system access or compromise, since these accounts are left active but will never be set up or logged into. Most users need to receive alerts for specific data of relevance to them, not to log in and access the system.*
>
> We offer an external email alert on a per Hot-Plate option, but is not provided for Automated large lists.

This is valuable on the hot-plate feature and will suffice for most of our day to day requests, but it is a functional gap that it cannot be used at the hot list level. It is a gap that does not exist in our current system, which means I have to identify a workable solution and make it available to our system users. There are a number of use cases for this beyond the first one mentioned, such as notifying patrol users of stolen vehicles in their area (installing and configuring TAS software on all of their computers is again wildly more cumbersome than enabling the LPR system to simply send them an email).

If you are looking for a workaround, the recommended solution is to have your IT setup an email distribution list of users to receive these alerts. Then we can configure a single User to configure the alerting options on a specific Alert type across a larger list.

This would be a good work around for a static user list. However this user list changes by incident and occasion and would not be under our LPR system administrators' control to update. It is not feasible to create multiple email distribution lists that are routinely changed or updated but that we can't control.

Jeremy, would you be willing to set up a call after the 4th to go over general updates and a few of the LEARN features like these that we are trying to navigate? This interface feels clunky and complicated, as we've mentioned before, and the mental gymnastics we've got to do to make it work is problematic. I know updates are in the works, but we are trying to migrate away from another vendor for issues like this, and I'm already getting push back from our small number of LEARN users that things are more difficult for them, not less. I've got to make this work, as this program is too important to fail. Your help would be immeasurably valuable to this process.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Investigative Services
Critical Incident Technical Investigations (CITI)
G L. c. 4.sec. 7 cl 26 (n)(security)

From: Jeremy Workman <jeremy.workman@motorolasolutions.com>
Sent: Monday, July 3, 2023 12:09 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Daniel Wilburn <daniel.wilburn@motorolasolutions.com>; Sean Derbyshire <sean.derbyshire@motorolasolutions.com>
Subject: Re: Hotlist Notification Setup

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

recognize the sender and know the content is safe.

Hello Noah,

It is advisable and CJIS best practices to have an associated account for each individual recipient for emails. We offer an external email alert on a per Hot-Plate option, but is not provided for Automated large lists.

If you are looking for a workaround, the recommended solution is to have your IT setup an email distribution list of users to receive these alerts. Then we can configure a single User to configure the alerting options on a specific Alert type across a larger list.

Example:

Create a list of users with your IT under single Email distribution list: MSI.ALPR.TerroristWatchlist@state.ma.us

Within LEARN, create an account with the Distro Email and assign desired Hotlist on load (or all agency users) and configure the "Alert Management" section to receive the desired alert/s and desired locations.

Regards,

On Mon, Jul 3, 2023 at 11:56 AM Pack, Noah (POL) <noah.pack@state.ma.us> wrote:

> Hey guys,
>
> I just spoke to support again about setting up hotlist notifications for another use case and was met with another sorry we can't do that. I'm starting to get concerned by the limitations of the notification features in LEARN.
>
> Could we set up a call in the near future to discuss some of the notification use cases here to see if we can work around or close these gaps? Thanks again for your time.
>
> Respectfully,
>
> Noah
>
> **Sergeant Noah H. Pack**
> Massachusetts State Police
> Division of Investigative Services
> Critical Incident Technical Investigations (CITI)
>
> ---
>
> **From:** Pack, Noah (POL)
> **Sent:** Monday, July 3, 2023 11:15 AM
> **To:** Daniel Wilburn <daniel.wilburn@motorolasolutions.com>; Jeremy Workman <jeremy.workman@motorolasolutions.com>

Cc: Sean Derbyshire <sean.derbyshire@motorolasolutions.com>
Subject: Hotlist Notification Setup

Another troubleshooting question for you guys:

We are looking to setup notifications to a group of email addresses to receive alerts from a specific category of hits from a specific device (and eventually set of devices). This is a common workflow for us across a variety of use cases, but it happens to be relevant now due to July 4th security operations.

Here's an example:

Goal: generate alerts to go out to email address of users without LEARN accounts
Alert type: one sub-category (i.e. terrorist watch list plates) from the automatically updated MA-NCIC hotlist file
Device restrictions: devices located in a certain region only; this is currently done by selecting specific devices but could also be done with a geo zone.

I called technical support to discuss this prior to reaching out to you guys, and they indicated they are unaware of how this can be done without setting up and configuring LEARN accounts and notification settings for all the recipients, which isn't a viable option for us, due at least in part to the complexity of setting up and configuring LEARN accounts and the associated alerts.

Thank you for allowing me to contact you guys directly, as you are exceptional problem solvers with this stuff, and I appreciate your help as we work to transition into making Vigilant work for MSP.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Investigative Services
Critical Incident Technical Investigations (CITI)

--
Jeremy Workman
Senior Product Manager, Vigilant
Mobile Video & Analytics **m:** [redacted]



This email and any attachments are for the authorized recipient's use only. If you receive this email in error, please immediately delete it from your system and notify the sender. You must not disclose, print, re-transmit, store, copy or rely on any part of this email and any attachments if you are not the authorized recipient. This email and any attachments are confidential and may contain confidential information and/or copyright material of Motorola Solutions, Inc.

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

--

Jeremy Workman
Senior Product Manager, Vigilant
Mobile Video & Analytics **m:** +[redacted]



This email and any attachments are for the authorized recipient's use only. If you receive this email in error, please immediately delete it from your system and notify the sender. You must not disclose, print, re-transmit, store, copy or rely on any part of this email and any attachments if you are not the authorized recipient. This email and any attachments are confidential and may contain confidential information and/or copyright material of Motorola Solutions, Inc.

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

From: Thibault, Amy (POL)
To: Smith, Eleanor (POL)
Subject: RE: HSOC LPR Training 9/14/2023
Date: Wednesday, September 6, 2023 10:23:00 AM

Great!

From: Smith, Eleanor (POL) <Eleanor.Smith@pol.state.ma.us>
Sent: Wednesday, September 6, 2023 10:23 AM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Subject: Re: HSOC LPR Training 9/14/2023

This was on my list of things to talk to Brooks about today. I'll let you know what I find out...

From: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Sent: Wednesday, September 6, 2023 10:15 AM
To: Smith, Eleanor (POL) <Eleanor.Smith@pol.state.ma.us>
Subject: FW: HSOC LPR Training 9/14/2023

Hi Elly,
I saw you weren't on here. Do you know if we're getting access to LEARN?
It looks like there is training below (I wonder if they can get them to stay past 3pm) and everyone will have to refresh themselves of TRF-11, especially the section below on Non-departmental ALPR Systems.

Use of Non-Departmental ALPR Systems
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.
Supervisors and analysts assigned to the Commonwealth Watch Center/Commonwealth Fusion Center and the ALPR Administrator may access non-departmental ALPR systems for official law enforcement purposes as authorized by this policy. 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, retention, and quality assurance standards than the Department's ALPR system. Members shall be mindful to preserve, export, or obtain copies of records or reports that are of known relevance to an incident or investigation prior to the expiry of the records.

From: Walczak, Ryan (POL) <ryan.walczak@pol.state.ma.us>
Sent: Tuesday, September 5, 2023 2:17 PM
To: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>

Cc: Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Rudolph, James (POL) <James.Rudolph@pol.state.ma.us>; Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>
Subject: Fw: HSOC LPR Training 9/14/2023

Good Afternoon,

We are meeting with Motorola on 9/14/2023 @0900HRS to approximately 1500HRS at GHQ HSOC. This will be a training given by Motorola in regards to the ALPR System "LEARN". Moving forward, this training will be mandatory for access to the system. There is currently no tentative date for a second training at this time. We strongly recommend that anyone in your unit who has access to, or uses the ALPR system in their current job title attend this training.

Respectfully,
Ryan

Sergeant Ryan Walczak #3731
Massachusetts State Police
Division Of Homeland Security and Preparedness
Technical Services Unit
G.L. c. 4.sec. 7.cl.26 (n)(security)
Email: Ryan.walczak@pol.state.ma.us

From: Walczak, Ryan (POL)
Sent: Tuesday, September 5, 2023 1:20 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Accepted: HSOC LPR Training
When: Thursday, September 14, 2023 9:00 AM-4:00 PM.
Where: 470 Worcester Road, Framingham, MA

From: Thibault, Amy (POL)
To: Smith, Eleanor (POL)
Subject: RE: HSOC LPR Training 9/14/2023
Date: Wednesday, September 6, 2023 10:25:00 AM

Oh. Makes sense. I knew it was vigilant but didn't know if it was the consumer data we supposedly had with the motorola project and couldn't purchase with our funds.

From: Smith, Eleanor (POL) <Eleanor.Smith@pol.state.ma.us>
Sent: Wednesday, September 6, 2023 10:25 AM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Subject: Re: HSOC LPR Training 9/14/2023

This is vigilant and will be replacing Boss 4...

From: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Sent: Wednesday, September 6, 2023 10:23 AM
To: Smith, Eleanor (POL) <Eleanor.Smith@pol.state.ma.us>
Subject: RE: HSOC LPR Training 9/14/2023

Great!

From: Smith, Eleanor (POL) <Eleanor.Smith@pol.state.ma.us>
Sent: Wednesday, September 6, 2023 10:23 AM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Subject: Re: HSOC LPR Training 9/14/2023

This was on my list of things to talk to Brooks about today. I'll let you know what I find out...

From: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Sent: Wednesday, September 6, 2023 10:15 AM
To: Smith, Eleanor (POL) <Eleanor.Smith@pol.state.ma.us>
Subject: FW: HSOC LPR Training 9/14/2023

Hi Elly,
I saw you weren't on here. Do you know if we're getting access to LEARN?
It looks like there is training below (I wonder if they can get them to stay past 3pm) and everyone will have to refresh themselves of TRF-11, especially the section below on Non-departmental ALPR Systems.

Use of Non-Departmental ALPR Systems
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.
Supervisors and analysts assigned to the Commonwealth Watch Center/Commonwealth Fusion Center and the ALPR Administrator may

access non-departmental ALPR systems for official law enforcement purposes as authorized by this policy. 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, retention, and quality assurance standards than the Department's ALPR system. Members shall be mindful to preserve, export, or obtain copies of records or reports that are of known relevance to an incident or investigation prior to the expiry of the records.

From: Walczak, Ryan (POL) <ryan.walczak@pol.state.ma.us>
Sent: Tuesday, September 5, 2023 2:17 PM
To: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Cc: Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Rudolph, James (POL) <James.Rudolph@pol.state.ma.us>; Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>
Subject: Fw: HSOC LPR Training 9/14/2023

Good Afternoon,

We are meeting with Motorola on 9/14/2023 @0900HRS to approximately 1500HRS at GHQ HSOC. This will be a training given by Motorola in regards to the ALPR System "LEARN". Moving forward, this training will be mandatory for access to the system. There is currently no tentative date for a second training at this time. We strongly recommend that anyone in your unit who has access to, or uses the ALPR system in their current job title attend this training.

Respectfully,
Ryan

Sergeant Ryan Walczak #3731
Massachusetts State Police
Division Of Homeland Security and Preparedness
Technical Services Unit
G.L. c. 4.sec. 7.cl.26 (n)(security)
Email: Ryan.walczak@pol.state.ma.us

From: Walczak, Ryan (POL)
Sent: Tuesday, September 5, 2023 1:20 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Accepted: HSOC LPR Training
When: Thursday, September 14, 2023 9:00 AM-4:00 PM.

Where: 470 Worcester Road, Framingham, MA

From: Pack, Noah (POL)
To: Cyr, Mark (POL)
Subject: Re: Language Draft
Date: Thursday, March 2, 2023 11:11:04 AM

From: Pack, Noah (POL)
Sent: Thursday, March 2, 2023 11:09 AM
To: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Subject: Language Draft

Sir, this is what I had in a draft (it is in the one I sent a few weeks ago) but was not in the one I sent them yesterday:

The Massachusetts Supreme Judicial Court has recognized that individuals have a reasonable expectation of privacy in the whole of their public movements (see *Commonwealth vs. McCarthy, 484 Mass. 493*). While the SJC indicated that the limited use of ALPR does not infringe upon a constitutional right, and therefore does not require a search warrant or other legal process, the widespread and long-term use of ALPR to investigate an individual may amount to a constitutional violation.

Combining this with their suggestions, it could look like:

The Massachusetts Supreme Judicial Court has recognized that individuals have a reasonable expectation of privacy in the whole of their public movements (see *Commonwealth vs. McCarthy, 484 Mass. 493*). While the SJC indicated that the limited use of ALPR does not infringe upon a constitutional right, and therefore does not require legal process, the extensive or long-term use of ALPR in active criminal investigations that do not involve exigent circumstances should be reviewed with a prosecutor of jurisdiction in the investigation for review of the potential necessity of a search warrant.

I'll review McCarthy again for other thoughts.

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: Cyr, Mark (POL)
Subject: Re: Language Draft
Date: Thursday, March 2, 2023 11:10:45 AM

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)
Sent: Thursday, March 2, 2023 11:09 AM
To: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Subject: Language Draft

Sir, this is what I had in a draft (it is in the one I sent a few weeks ago) but was not in the one I sent them yesterday:

The Massachusetts Supreme Judicial Court has recognized that individuals have a reasonable expectation of privacy in the whole of their public movements (see *Commonwealth vs. McCarthy, 484 Mass. 493*). While the SJC indicated that the limited use of ALPR does not infringe upon a constitutional right, and therefore does not require a search warrant or other legal process, the widespread and long-term use of ALPR to investigate an individual may amount to a constitutional violation.

Combining this with their suggestions, it could look like:

The Massachusetts Supreme Judicial Court has recognized that individuals have a reasonable expectation of privacy in the whole of their public movements (see *Commonwealth vs. McCarthy, 484 Mass. 493*). While the SJC indicated that the limited use of ALPR does not infringe upon a constitutional right, and therefore does not require legal process, the extensive or long-term use of ALPR in active criminal investigations that do not involve exigent circumstances should be reviewed with a prosecutor of jurisdiction in the investigation for review of the potential necessity of a search warrant.

I'll review McCarthy again for other thoughts.

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: Cyr, Mark (POL)
To: Pack, Noah (POL)
Subject: Re: Language Draft
Date: Thursday, March 2, 2023 11:52:26 AM

Received. That combination language may be a decent middle ground...

Mark

Lieutenant Colonel Mark D. Cyr #2728
Massachusetts State Police
Division Commander
Division of Homeland Security and Preparedness
508-988-7301 (office)
[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: Thursday, March 2, 2023 11:09 AM
To: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Subject: Language Draft

Sir, this is what I had in a draft (it is in the one I sent a few weeks ago) but was not in the one I sent them yesterday:

The Massachusetts Supreme Judicial Court has recognized that individuals have a reasonable expectation of privacy in the whole of their public movements (see *Commonwealth vs. McCarthy, 484 Mass. 493*). While the SJC indicated that the limited use of ALPR does not infringe upon a constitutional right, and therefore does not require a search warrant or other legal process, the widespread and long-term use of ALPR to investigate an individual may amount to a constitutional violation.

Combining this with their suggestions, it could look like:

The Massachusetts Supreme Judicial Court has recognized that individuals have a reasonable expectation of privacy in the whole of their public movements (see *Commonwealth vs. McCarthy, 484 Mass. 493*). While the SJC indicated that the limited use of ALPR does not infringe upon a constitutional right, and therefore does not require legal process, the extensive or long-term use of ALPR in active criminal investigations that do not involve exigent circumstances should be reviewed with a prosecutor of jurisdiction in the investigation for review of the potential necessity of a search warrant.

I'll review McCarthy again for other thoughts.

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: Quinn, Dermot (POL)
To: Walczak, Ryan (POL); Boutwell, Brian (POL)
Cc: Pack, Noah (POL); George, Michael (POL)
Subject: RE: MSP ALPR System
Date: Monday, October 23, 2023 12:55:44 PM

Thank you sirs.

Will the one year of historical data be available through Vigilant or is this a fresh start?

Respectfully,

Dermot

Dermot J. Quinn #1765
Criminal Information Section
Division of Homeland Security
Massachusetts State Police
617 590-1450
dermot.quinn@pol.state.ma.us
(Ret Lt Col MSP)

From: Walczak, Ryan (POL) <ryan.walczak@pol.state.ma.us>
Sent: Monday, October 23, 2023 12:46 PM
To: Boutwell, Brian (POL) <Brian.Boutwell@pol.state.ma.us>
Cc: Pack, Noah (POL) <noah.pack@pol.state.ma.us>; George, Michael (POL) <Michael.George@pol.state.ma.us>
Subject: MSP ALPR System

Good Morning,

Please be advised that the Department is transitioning to a different LPR system. If you are receiving this email, you currently have an account in the Department's legacy LPR system. The legacy system will effectively be discontinued as of close of

business, today Monday, October 23, 2023.

If you do not have a current account with the Departments new LPR system, you can contact the Commonwealth Watch Center (fusion@pol.state.ma.us) with all hotlist requests. Please refer to MSP Policy TRF-11 for guidance when requesting a hotlist. At this time, the Department is working to try and set up a future training date to allow users access into the new and current MSP system. If you have any questions or concerns please reach out to me directly.

Respectfully,

Sergeant Ryan Walczak #3731
Massachusetts State Police
Division Of Homeland Security and Preparedness
Technical Services Unit
G.L. c. 4.sec. 7.cl.26 (n)(security)
Email: Ryan.walczak@pol.state.ma.us

From: Driscoll, Elaine (EPS)
To: Procopio, David (POL)
Subject: Re: Proposed statement/background + policy
Date: Friday, October 20, 2023 11:36:26 AM

Ok

Sent from my iPhone

> On Oct 20, 2023, at 11:25 AM, Procopio, David (POL) <david.procopio@pol.state.ma.us> wrote:
>
> Yes would include it.
>
> Fyi – got pulled off any further research on that topic in order to write remarks for Colonel for next week's Women in Law Enforcement conference.
>
> Dave Procopio
> Director, Media Relations Unit
> Massachusetts State Police
>
> ---
>
> **From:** Driscoll, Elaine (EPS) <Elaine.Driscoll@mass.gov>
> **Sent:** Friday, October 20, 2023 11:24 AM
> **To:** Procopio, David (POL) <david.procopio@pol.state.ma.us>
> **Subject:** Re: Proposed statement/background + policy
>
> Ok great. And you would include the policy? I'm headed to a meeting with Gov's now and will seek approval
>
> Sent from my iPhone
>
> > On Oct 20, 2023, at 10:19 AM, Procopio, David (POL) <david.procopio@pol.state.ma.us> wrote:
> >
> > Here is a proposed statement and two background points, plus the policy.
> > I don't have any answers yet on numbers of times used.
> >
> > Statement:
> > "The ability to query information about vehicles connected to serious crimes, through both the MSP's automated license plate readers and the DOT's tolling gantries, is a valuable tool to assist in capturing dangerous offenders, securing justice for their victims, and protecting public safety

and homeland security. The MSP utilizes both systems judiciously and in accordance with state and federal laws and Constitutional rights of individuals."
-Me

Background:
-Use of the MSP's ALPR system is governed by a rigorous Departmental policy, TRF-11 (copy attached to this response).
-MSP investigators do not have direct access to the DOT gantry information, and request such data from the DOT's legal division via a thorough process that ensures all relevant criteria and safeguards are met.

Dave Procopio
Director, Media Relations Unit
Massachusetts State Police
<image001.png>

<TRF-11.pdf>

From: Arunima Choudhary
To: Parr, Robert (POL)
Subject: Request to connect for discussing GeoShield RTCC Solution.
Date: Thursday, May 25, 2023 10:50:13 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.

Dear Robert,

Hope this email finds you well.

I have been attempting to contact you several times in the past especially in my last mail on 2nd May'23 which elaborated our GeoShield RTCC Solution:

1. Uniquely connects multiple data sources like CAD, RMS, AVL, ALPR, etc.
2. Re-Designed Dashboard for Immersive Experience & Quick Access.
3. City Monitoring and Situational Awareness.
4. Advanced Mapping and Spatial Analytics.

My purpose in reaching out to you today is to inquire whether you anticipate a need for the RTCC Solution mentioned above within coming years.

Would like to offer our assistance by providing you a one-on-one interactive session with our experts to give you a better understanding of the potential scope of the Real-Time Crime Center initiatives for 2023-2024.

To facilitate this, would propose scheduling a call at a mutually convenient time.

Look forward to hearing from you soon.

Thank you.

Cheers,
Arunima Choudhary
(630) 214 – 9787
arunima.choudhary@spatialitics.com

From: Arunima Choudhary
To: LaBelle, Keri (POL)
Subject: Request to connect for discussing GeoShield RTCC Solution.
Date: Thursday, May 25, 2023 10:50:12 AM

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

Dear Keri,

Hope this email finds you well.

I have been attempting to contact you several times in the past especially in my last mail on 2nd May'23 which elaborated our GeoShield RTCC Solution:

1. Uniquely connects multiple data sources like CAD, RMS, AVL, ALPR, etc.
2. Re-Designed Dashboard for Immersive Experience & Quick Access.
3. City Monitoring and Situational Awareness.
4. Advanced Mapping and Spatial Analytics.

My purpose in reaching out to you today is to inquire whether you anticipate a need for the RTCC Solution mentioned above within coming years.

Would like to offer our assistance by providing you a one-on-one interactive session with our experts to give you a better understanding of the potential scope of the Real-Time Crime Center initiatives for 2023-2024.

To facilitate this, would propose scheduling a call at a mutually convenient time.

Look forward to hearing from you soon.

Thank you.

Cheers,
Arunima Choudhary
(630) 214 – 9787
arunima.choudhary@spatialitics.com

From: Arunima Choudhary
To: Short, Donald (POL)
Subject: Request to connect for discussing GeoShield RTCC Solution.
Date: Thursday, May 25, 2023 10:50:07 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.

Dear Donald,

Hope this email finds you well.

I have been attempting to contact you several times in the past especially in my last mail on 2nd May'23 which elaborated our GeoShield RTCC Solution:

1. Uniquely connects multiple data sources like CAD, RMS, AVL, ALPR, etc.
2. Re-Designed Dashboard for Immersive Experience & Quick Access.
3. City Monitoring and Situational Awareness.
4. Advanced Mapping and Spatial Analytics.

My purpose in reaching out to you today is to inquire whether you anticipate a need for the RTCC Solution mentioned above within coming years.

Would like to offer our assistance by providing you a one-on-one interactive session with our experts to give you a better understanding of the potential scope of the Real-Time Crime Center initiatives for 2023-2024.

To facilitate this, would propose scheduling a call at a mutually convenient time.

Look forward to hearing from you soon.

Thank you.

Cheers,
Arunima Choudhary
(630) 214 – 9787
arunima.choudhary@spatialitics.com

From: Arunima Choudhary
To: zzHodgdon, Sean (POL)
Subject: Request to connect for discussing GeoShield RTCC Solution.
Date: Thursday, May 25, 2023 10:50:00 AM

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

Dear Sean,

Hope this email finds you well.

I have been attempting to contact you several times in the past especially in my last mail on 2nd May'23 which elaborated our GeoShield RTCC Solution:

1. Uniquely connects multiple data sources like CAD, RMS, AVL, ALPR, etc.
2. Re-Designed Dashboard for Immersive Experience & Quick Access.
3. City Monitoring and Situational Awareness.
4. Advanced Mapping and Spatial Analytics.

My purpose in reaching out to you today is to inquire whether you anticipate a need for the RTCC Solution mentioned above within coming years.

Would like to offer our assistance by providing you a one-on-one interactive session with our experts to give you a better understanding of the potential scope of the Real-Time Crime Center initiatives for 2023-2024.

To facilitate this, would propose scheduling a call at a mutually convenient time.

Look forward to hearing from you soon.

Thank you.

Cheers,
Arunima Choudhary
(630) 214 – 9787
arunima.choudhary@spatialitics.com

From: Arunima Choudhary
To: Connors, Brian (POL)
Subject: Request to connect for discussing GeoShield RTCC Solution.
Date: Thursday, May 25, 2023 10:50:17 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.

Dear Brian,

Hope this email finds you well.

I have been attempting to contact you several times in the past especially in my last mail on 2nd May'23 which elaborated our GeoShield RTCC Solution:

1. Uniquely connects multiple data sources like CAD, RMS, AVL, ALPR, etc.
2. Re-Designed Dashboard for Immersive Experience & Quick Access.
3. City Monitoring and Situational Awareness.
4. Advanced Mapping and Spatial Analytics.

My purpose in reaching out to you today is to inquire whether you anticipate a need for the RTCC Solution mentioned above within coming years.

Would like to offer our assistance by providing you a one-on-one interactive session with our experts to give you a better understanding of the potential scope of the Real-Time Crime Center initiatives for 2023-2024.

To facilitate this, would propose scheduling a call at a mutually convenient time.

Look forward to hearing from you soon.

Thank you.

Cheers,
Arunima Choudhary
(630) 214 – 9787
arunima.choudhary@spatialitics.com

From: Genetec newsletter
To: Mcnamara, Sean (POL)
Subject: Sean, see why IIoT matters
Date: Thursday, July 27, 2023 1:02:26 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.

Connecting the dots from Genetec

Hi Sean,

Everything you ever wanted to know about the Industrial Internet of Things (IIoT) is here! We even included real-life customer examples to give you ideas about how your team can connect IIoT sensors to get more from your physical security system.

Happy reading,

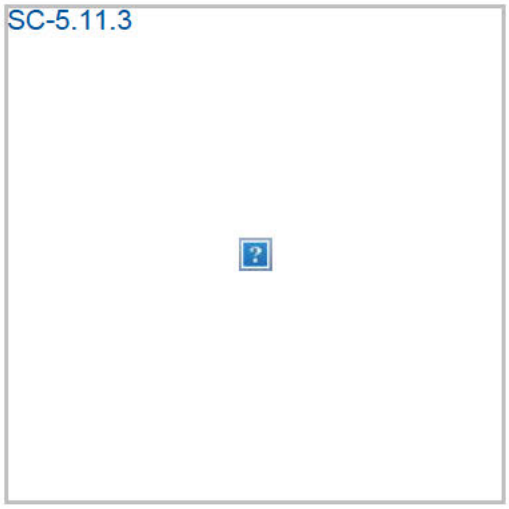
Julie Cadieux, **Senior Editor**
jcadieux@genetec.com

Product updates

Security Center 5.11.3

The latest release simplifies password management, allows you to schedule automatic firmware updates, and create dashboard customizations.

Read →





Take SIP calls on the go

The new version of Sipelia™ turns your mobile phone or tablet into a powerful security communication device.

← Read

Want better ALPR capture rates?

AutoVu™ Sharp Z3, our ALPR solution, has major new features

like stereoscopy, analytics, and dual exposure.

Read →

ALPR-AutoVu

Industrial Internet of Things

IoT-IIoT

Why IIoT matters

Find out how cloud, cybersecurity, unification, and AI impact the success of your IIoT journey.

← Read

Tips & tricks

TechDoc Hub

Check out the Genetec™ Mobile Getting Started Guide to learn how to perform Security Desk monitoring functions from your smartphone.

Read →

Genetec-mobile

people-detection

How does YOLO work?

Learn about object detection in video analytics, and why everyone's talking about the YOLO algorithm.

← Read

ClearID

Looking for ways to ensure security compliance and audit readiness?

Discover a simplified auditing process that allows you to schedule or manually launch access reviews through a self-service portal.

Simplify the audit process with ClearID

Get the updates you need

.ıail icon

Select products of interest, preferred language, and more in our email preference center.

Manage your preferences →

View this online · Manage your preferences · Unsubscribe

Genetec Inc.
2280 Alfred-Nobel Blvd., Montreal, QC H4S 2A4 Canada

© 2023 Genetec Inc. TM trademark of Genetec Inc.

From: Police Fleet Professional Magazine
To: zzFernandes, Paul (POL)
Subject: September 2023 eNews End of Month
Date: Friday, September 29, 2023 5:26:09 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.

Logo

Sponsored by General Tire & Tufloc

INDUSTRY NEWS

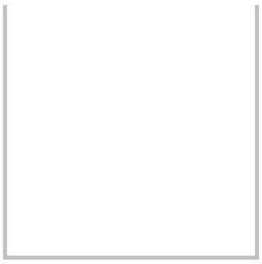
Sartell Adds Military Themed Squad Car to the Fleet

The Sartell Police Department (MN) unveiled a new, military service-themed squad car that will be used by police officers who are also military veterans.

The eye-catching design helps bring attention to the local organizations working with veterans fighting PTSD and working to prevent soldier and first responder suicide.

The emblems of the Invisible Wounds Project, Soldier's 6, and 23rd Veteran programs are prominently displayed on the squad car.

Sartell Police Chief Brandon Silgjord says he's honored to have the vehicle on active patrol and hopes it's a symbol to the community that no one fights alone.





Click for Full Story

Claremont PD Rolls Out New Electric Cruiser



The Claremont Police Department (NH) is showing off some new digs.

The department now has a fully electric F150 pickup truck in it's fleet, donated by the local dealership Ford of Claremont.

The department says it is the first municipality in the Northeast to use this type of vehicle on patrol. The Chief says it's a positive change for the department.

"You know we haven't had to put gas in the car so we have saved money right there. Right out of the gate. So, it is interesting, it is definitely something that we are getting used to," Chief Brent Wilmot said. "I think it is something that this profession, law enforcement in general will be getting used to in the coming years."

Ford of Claremont also donated a charging station and emergency lights. This is the second vehicle the business has donated to the department in recent years.

Click for Full Story

GM Presents In-Depth Overview Of 2024 Chevy Blazer EV Police Pursuit Vehicle



The 2024 Chevy Blazer EV was unveiled in July of 2022, with GM pulling the sheets on a new midsize crossover propelled by The General's latest all-electric vehicle technology.

While the 2024 Chevy Blazer EV will be available to civilians in a wide variety of configurations and trim levels, Chevy will also offer a Police Pursuit Vehicle (PPV) variant to law enforcement. Now, we're getting a thorough look at what the new 2024 Chevy Blazer EV PPV has to offer thanks to a recently released video.

Clocking in at 12 minutes and 26 seconds, the video provides an overview of all the features of the first pursuit-rated EV based on the GM Ultium platform. Highlights of the 2024 Chevy Blazer EV PPV include a 400-volt all-wheel-drive propulsion system. Maximum output is set at 498 horsepower and 531 pound-feet of torque. There's also an even 50/50 front-to-rear weight distribution for enhanced handling, while the onboard 105 kWh battery provides an estimated 250 miles of range on a full charge.

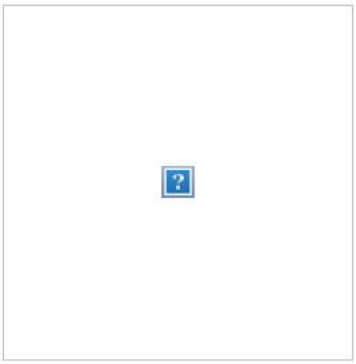
Upgraded heavy duty suspension and six-piston Brembo front brake calipers (matched to 15.3-inch rotors) help to handle the heft, while a set of underbody

skid plates protect the bits under the body. The police crossover also rides on 20-inch steel wheels wrapped in Firestone Firehawk Pursuit tires.

Click for Full Story

ADVERTORIAL | Stalker Radar

The LidarCam 2: Where Cutting-Edge Lidar Speed Enforcement Meets Undeniable Photo and Video Evidence Capture



Automatically collect a video + multiple high-resolution photos every time you capture a traffic violation. Built-in License Plate Reading Technology (ANPR/ALPR) can automatically check for wanted plates or other violations. Hand-held or mounted to a tripod, the Stalker LidarCam 2 is the next generation of photo enforcement.

Up to 1TB of internal storage allows you to save multiple days-worth of evidence onboard before you upload them into the included secure PC-based Evidence Manager software for viewing, processing, and sharing. AES-256 encryption comes standard, keeping your data secure.

The LidarCam 2 is equipped with built-in GPS, USB-C, and Wi-Fi, with optional 4G-LTE cellular connection available. Fully-remote wireless operation in real time on any platform - phone, tablet, or desktop - with no proprietary apps needed. Learn more at StalkerRadar.com/video-lidar or call us today at 1-800-STALKER.

PRODUCTS

Underseat Storage System From Pro-gard Products



Pro-gard Products LLC introduces the Under Seat Storage System for F-150 and Super Duty Crew Cabs, catering to law enforcement storage needs.

This advanced solution optimizes cargo space for equipment and weapons while ensuring secure, organized storage. Its dual compartments offer versatility with a removable divider and locking latches for weapon security. Constructed from durable steel with a textured black powder coat finish, it includes a rubber mat-lined floor for protection. Installation is effortless, attaching seamlessly to OEM holes without drilling.

Pro-gard's commitment to enhancing officer efficiency and safety shines throughout this innovative system.

Click for Pro-gard Products

Do you have news to share?

Please contact National Director, Kirk Moen: kmoen@signalbusinessgroup.com for more information.

Signal Business Group LLC
PO Box 3157, Bluffton, SC 29910-3157
P: 224-458-1123
E: info@signalbusinessgroup.com

Visit Us | 2023 Media Kit | See you in Forth Worth, TX 2024!

If you wish to unsubscribe from our newsletter, click here

From: Police Fleet Professional Magazine
To: zzBrenner, Karl (POL)
Subject: September 2023 eNews End of Month
Date: Friday, September 29, 2023 5:25:12 PM

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

Logo

Sponsored by General Tire & Tufloc

INDUSTRY NEWS

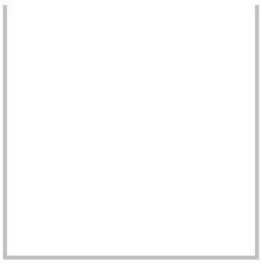
Sartell Adds Military Themed Squad Car to the Fleet

The Sartell Police Department (MN) unveiled a new, military service-themed squad car that will be used by police officers who are also military veterans.

The eye-catching design helps bring attention to the local organizations working with veterans fighting PTSD and working to prevent soldier and first responder suicide.

The emblems of the Invisible Wounds Project, Soldier's 6, and 23rd Veteran programs are prominently displayed on the squad car.

Sartell Police Chief Brandon Silgjord says he's honored to have the vehicle on active patrol and hopes it's a symbol to the community that no one fights alone.





Click for Full Story

Claremont PD Rolls Out New Electric Cruiser



The Claremont Police Department (NH) is showing off some new digs.

The department now has a fully electric F150 pickup truck in it's fleet, donated by the local dealership Ford of Claremont.

The department says it is the first municipality in the Northeast to use this type of vehicle on patrol. The Chief says it's a positive change for the department.

"You know we haven't had to put gas in the car so we have saved money right there. Right out of the gate. So, it is interesting, it is definitely something that we are getting used to," Chief Brent Wilmot said. "I think it is something that this profession, law enforcement in general will be getting used to in the coming years."

Ford of Claremont also donated a charging station and emergency lights. This is the second vehicle the business has donated to the department in recent years.

Click for Full Story

GM Presents In-Depth Overview Of 2024 Chevy Blazer EV Police Pursuit Vehicle



The 2024 Chevy Blazer EV was unveiled in July of 2022, with GM pulling the sheets on a new midsize crossover propelled by The General's latest all-electric vehicle technology.

While the 2024 Chevy Blazer EV will be available to civilians in a wide variety of configurations and trim levels, Chevy will also offer a Police Pursuit Vehicle (PPV) variant to law enforcement. Now, we're getting a thorough look at what the new 2024 Chevy Blazer EV PPV has to offer thanks to a recently released video.

Clocking in at 12 minutes and 26 seconds, the video provides an overview of all the features of the first pursuit-rated EV based on the GM Ultium platform. Highlights of the 2024 Chevy Blazer EV PPV include a 400-volt all-wheel-drive propulsion system. Maximum output is set at 498 horsepower and 531 pound-feet of torque. There's also an even 50/50 front-to-rear weight distribution for enhanced handling, while the onboard 105 kWh battery provides an estimated 250 miles of range on a full charge.

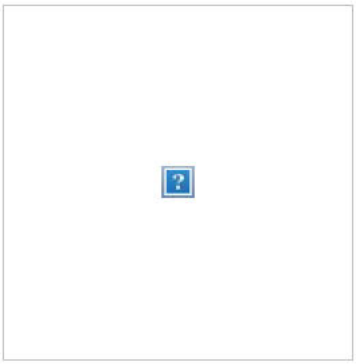
Upgraded heavy duty suspension and six-piston Brembo front brake calipers (matched to 15.3-inch rotors) help to handle the heft, while a set of underbody

skid plates protect the bits under the body. The police crossover also rides on 20-inch steel wheels wrapped in Firestone Firehawk Pursuit tires.

Click for Full Story

ADVERTORIAL | Stalker Radar

The LidarCam 2: Where Cutting-Edge Lidar Speed Enforcement Meets Undeniable Photo and Video Evidence Capture



Automatically collect a video + multiple high-resolution photos every time you capture a traffic violation. Built-in License Plate Reading Technology (ANPR/ALPR) can automatically check for wanted plates or other violations. Hand-held or mounted to a tripod, the Stalker LidarCam 2 is the next generation of photo enforcement.

Up to 1TB of internal storage allows you to save multiple days-worth of evidence onboard before you upload them into the included secure PC-based Evidence Manager software for viewing, processing, and sharing. AES-256 encryption comes standard, keeping your data secure.

The LidarCam 2 is equipped with built-in GPS, USB-C, and Wi-Fi, with optional 4G-LTE cellular connection available. Fully-remote wireless operation in real time on any platform - phone, tablet, or desktop - with no proprietary apps needed. Learn more at StalkerRadar.com/video-lidar or call us today at 1-800-STALKER.

PRODUCTS

Underseat Storage System From Pro-gard Products



Pro-gard Products LLC introduces the Under Seat Storage System for F-150 and Super Duty Crew Cabs, catering to law enforcement storage needs.

This advanced solution optimizes cargo space for equipment and weapons while ensuring secure, organized storage. Its dual compartments offer versatility with a removable divider and locking latches for weapon security. Constructed from durable steel with a textured black powder coat finish, it includes a rubber mat-lined floor for protection. Installation is effortless, attaching seamlessly to OEM holes without drilling.

Pro-gard's commitment to enhancing officer efficiency and safety shines throughout this innovative system.

Click for Pro-gard Products

Do you have news to share?

Please contact National Director, Kirk Moen: kmoen@signalbusinessgroup.com for more information.

Signal Business Group LLC
PO Box 3157, Bluffton, SC 29910-3157
P: 224-458-1123
E: info@signalbusinessgroup.com

Visit Us | 2023 Media Kit | See you in Forth Worth, TX 2024!

If you wish to unsubscribe from our newsletter, click here

From: Police Fleet Professional Magazine
To: Robles, Francis Jr. (POL)
Subject: September 2023 eNews End of Month
Date: Friday, September 29, 2023 5:18:17 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.

Logo

Sponsored by General Tire & Tufloc

INDUSTRY NEWS

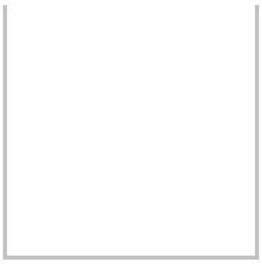
Sartell Adds Military Themed Squad Car to the Fleet

The Sartell Police Department (MN) unveiled a new, military service-themed squad car that will be used by police officers who are also military veterans.

The eye-catching design helps bring attention to the local organizations working with veterans fighting PTSD and working to prevent soldier and first responder suicide.

The emblems of the Invisible Wounds Project, Soldier's 6, and 23rd Veteran programs are prominently displayed on the squad car.

Sartell Police Chief Brandon Silgjord says he's honored to have the vehicle on active patrol and hopes it's a symbol to the community that no one fights alone.





Click for Full Story

Claremont PD Rolls Out New Electric Cruiser



The Claremont Police Department (NH) is showing off some new digs.

The department now has a fully electric F150 pickup truck in it's fleet, donated by the local dealership Ford of Claremont.

The department says it is the first municipality in the Northeast to use this type of vehicle on patrol. The Chief says it's a positive change for the department.

"You know we haven't had to put gas in the car so we have saved money right there. Right out of the gate. So, it is interesting, it is definitely something that we are getting used to," Chief Brent Wilmot said. "I think it is something that this profession, law enforcement in general will be getting used to in the coming years."

Ford of Claremont also donated a charging station and emergency lights. This is the second vehicle the business has donated to the department in recent years.

Click for Full Story

GM Presents In-Depth Overview Of 2024 Chevy Blazer EV Police Pursuit Vehicle



The 2024 Chevy Blazer EV was unveiled in July of 2022, with GM pulling the sheets on a new midsize crossover propelled by The General's latest all-electric vehicle technology.

While the 2024 Chevy Blazer EV will be available to civilians in a wide variety of configurations and trim levels, Chevy will also offer a Police Pursuit Vehicle (PPV) variant to law enforcement. Now, we're getting a thorough look at what the new 2024 Chevy Blazer EV PPV has to offer thanks to a recently released video.

Clocking in at 12 minutes and 26 seconds, the video provides an overview of all the features of the first pursuit-rated EV based on the GM Ultium platform. Highlights of the 2024 Chevy Blazer EV PPV include a 400-volt all-wheel-drive propulsion system. Maximum output is set at 498 horsepower and 531 pound-feet of torque. There's also an even 50/50 front-to-rear weight distribution for enhanced handling, while the onboard 105 kWh battery provides an estimated 250 miles of range on a full charge.

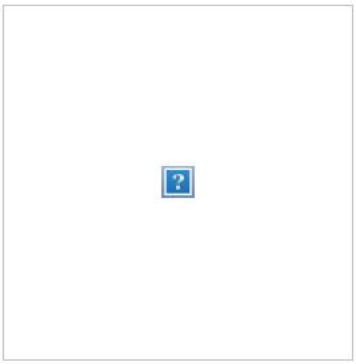
Upgraded heavy duty suspension and six-piston Brembo front brake calipers (matched to 15.3-inch rotors) help to handle the heft, while a set of underbody

skid plates protect the bits under the body. The police crossover also rides on 20-inch steel wheels wrapped in Firestone Firehawk Pursuit tires.

Click for Full Story

ADVERTORIAL | Stalker Radar

The LidarCam 2: Where Cutting-Edge Lidar Speed Enforcement Meets Undeniable Photo and Video Evidence Capture



Automatically collect a video + multiple high-resolution photos every time you capture a traffic violation. Built-in License Plate Reading Technology (ANPR/ALPR) can automatically check for wanted plates or other violations. Hand-held or mounted to a tripod, the Stalker LidarCam 2 is the next generation of photo enforcement.

Up to 1TB of internal storage allows you to save multiple days-worth of evidence onboard before you upload them into the included secure PC-based Evidence Manager software for viewing, processing, and sharing. AES-256 encryption comes standard, keeping your data secure.

The LidarCam 2 is equipped with built-in GPS, USB-C, and Wi-Fi, with optional 4G-LTE cellular connection available. Fully-remote wireless operation in real time on any platform - phone, tablet, or desktop - with no proprietary apps needed. Learn more at StalkerRadar.com/video-lidar or call us today at 1-800-STALKER.

PRODUCTS

Underseat Storage System From Pro-gard Products



Pro-gard Products LLC introduces the Under Seat Storage System for F-150 and Super Duty Crew Cabs, catering to law enforcement storage needs.

This advanced solution optimizes cargo space for equipment and weapons while ensuring secure, organized storage. Its dual compartments offer versatility with a removable divider and locking latches for weapon security. Constructed from durable steel with a textured black powder coat finish, it includes a rubber mat-lined floor for protection. Installation is effortless, attaching seamlessly to OEM holes without drilling.

Pro-gard's commitment to enhancing officer efficiency and safety shines throughout this innovative system.

Click for Pro-gard Products

Do you have news to share?

Please contact National Director, Kirk Moen: kmoen@signalbusinessgroup.com for more information.

Signal Business Group LLC
PO Box 3157, Bluffton, SC 29910-3157
P: 224-458-1123
E: info@signalbusinessgroup.com

Visit Us | 2023 Media Kit | See you in Forth Worth, TX 2024!

If you wish to unsubscribe from our newsletter, click here

From: Police Fleet Professional Magazine
To: Daige, Andrew (POL)
Subject: September 2023 eNews End of Month
Date: Friday, September 29, 2023 5:18:15 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.

Logo

Sponsored by General Tire & Tufloc

INDUSTRY NEWS

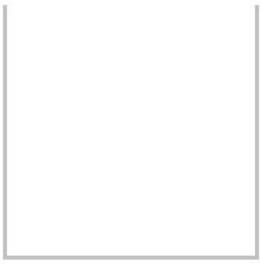
Sartell Adds Military Themed Squad Car to the Fleet

The Sartell Police Department (MN) unveiled a new, military service-themed squad car that will be used by police officers who are also military veterans.

The eye-catching design helps bring attention to the local organizations working with veterans fighting PTSD and working to prevent soldier and first responder suicide.

The emblems of the Invisible Wounds Project, Soldier's 6, and 23rd Veteran programs are prominently displayed on the squad car.

Sartell Police Chief Brandon Silgjord says he's honored to have the vehicle on active patrol and hopes it's a symbol to the community that no one fights alone.





Click for Full Story

Claremont PD Rolls Out New Electric Cruiser



The Claremont Police Department (NH) is showing off some new digs.

The department now has a fully electric F150 pickup truck in it's fleet, donated by the local dealership Ford of Claremont.

The department says it is the first municipality in the Northeast to use this type of vehicle on patrol. The Chief says it's a positive change for the department.

"You know we haven't had to put gas in the car so we have saved money right there. Right out of the gate. So, it is interesting, it is definitely something that we are getting used to," Chief Brent Wilmot said. "I think it is something that this profession, law enforcement in general will be getting used to in the coming years."

Ford of Claremont also donated a charging station and emergency lights. This is the second vehicle the business has donated to the department in recent years.

Click for Full Story

GM Presents In-Depth Overview Of 2024 Chevy Blazer EV Police Pursuit Vehicle



The 2024 Chevy Blazer EV was unveiled in July of 2022, with GM pulling the sheets on a new midsize crossover propelled by The General's latest all-electric vehicle technology.

While the 2024 Chevy Blazer EV will be available to civilians in a wide variety of configurations and trim levels, Chevy will also offer a Police Pursuit Vehicle (PPV) variant to law enforcement. Now, we're getting a thorough look at what the new 2024 Chevy Blazer EV PPV has to offer thanks to a recently released video.

Clocking in at 12 minutes and 26 seconds, the video provides an overview of all the features of the first pursuit-rated EV based on the GM Ultium platform. Highlights of the 2024 Chevy Blazer EV PPV include a 400-volt all-wheel-drive propulsion system. Maximum output is set at 498 horsepower and 531 pound-feet of torque. There's also an even 50/50 front-to-rear weight distribution for enhanced handling, while the onboard 105 kWh battery provides an estimated 250 miles of range on a full charge.

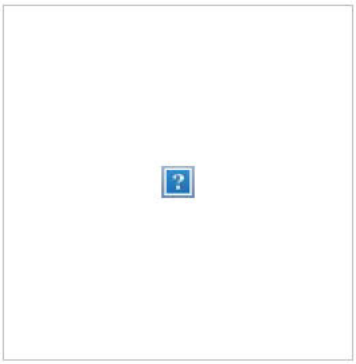
Upgraded heavy duty suspension and six-piston Brembo front brake calipers (matched to 15.3-inch rotors) help to handle the heft, while a set of underbody

skid plates protect the bits under the body. The police crossover also rides on 20-inch steel wheels wrapped in Firestone Firehawk Pursuit tires.

Click for Full Story

ADVERTORIAL | Stalker Radar

The LidarCam 2: Where Cutting-Edge Lidar Speed Enforcement Meets Undeniable Photo and Video Evidence Capture



Automatically collect a video + multiple high-resolution photos every time you capture a traffic violation. Built-in License Plate Reading Technology (ANPR/ALPR) can automatically check for wanted plates or other violations. Hand-held or mounted to a tripod, the Stalker LidarCam 2 is the next generation of photo enforcement.

Up to 1TB of internal storage allows you to save multiple days-worth of evidence onboard before you upload them into the included secure PC-based Evidence Manager software for viewing, processing, and sharing. AES-256 encryption comes standard, keeping your data secure.

The LidarCam 2 is equipped with built-in GPS, USB-C, and Wi-Fi, with optional 4G-LTE cellular connection available. Fully-remote wireless operation in real time on any platform - phone, tablet, or desktop - with no proprietary apps needed. Learn more at StalkerRadar.com/video-lidar or call us today at 1-800-STALKER.

PRODUCTS

Underseat Storage System From Pro-gard Products



Pro-gard Products LLC introduces the Under Seat Storage System for F-150 and Super Duty Crew Cabs, catering to law enforcement storage needs.

This advanced solution optimizes cargo space for equipment and weapons while ensuring secure, organized storage. Its dual compartments offer versatility with a removable divider and locking latches for weapon security. Constructed from durable steel with a textured black powder coat finish, it includes a rubber mat-lined floor for protection. Installation is effortless, attaching seamlessly to OEM holes without drilling.

Pro-gard's commitment to enhancing officer efficiency and safety shines throughout this innovative system.

Click for Pro-gard Products

Do you have news to share?

Please contact National Director, Kirk Moen: kmoen@signalbusinessgroup.com for more information.

Signal Business Group LLC
PO Box 3157, Bluffton, SC 29910-3157
P: 224-458-1123
E: info@signalbusinessgroup.com

Visit Us | 2023 Media Kit | See you in Forth Worth, TX 2024!

If you wish to unsubscribe from our newsletter, click here

From: Police Fleet Professional Magazine
To: Robles, Francis Jr. (POL)
Subject: September 2023 eNews End of Month
Date: Friday, September 29, 2023 5:18:15 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.

Logo

Sponsored by General Tire & Tufloc

INDUSTRY NEWS

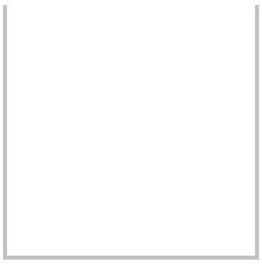
Sartell Adds Military Themed Squad Car to the Fleet

The Sartell Police Department (MN) unveiled a new, military service-themed squad car that will be used by police officers who are also military veterans.

The eye-catching design helps bring attention to the local organizations working with veterans fighting PTSD and working to prevent soldier and first responder suicide.

The emblems of the Invisible Wounds Project, Soldier's 6, and 23rd Veteran programs are prominently displayed on the squad car.

Sartell Police Chief Brandon Silgjord says he's honored to have the vehicle on active patrol and hopes it's a symbol to the community that no one fights alone.





Click for Full Story

Claremont PD Rolls Out New Electric Cruiser



The Claremont Police Department (NH) is showing off some new digs.

The department now has a fully electric F150 pickup truck in it's fleet, donated by the local dealership Ford of Claremont.

The department says it is the first municipality in the Northeast to use this type of vehicle on patrol. The Chief says it's a positive change for the department.

"You know we haven't had to put gas in the car so we have saved money right there. Right out of the gate. So, it is interesting, it is definitely something that we are getting used to," Chief Brent Wilmot said. "I think it is something that this profession, law enforcement in general will be getting used to in the coming years."

Ford of Claremont also donated a charging station and emergency lights. This is the second vehicle the business has donated to the department in recent years.

Click for Full Story

GM Presents In-Depth Overview Of 2024 Chevy Blazer EV Police Pursuit Vehicle



The 2024 Chevy Blazer EV was unveiled in July of 2022, with GM pulling the sheets on a new midsize crossover propelled by The General's latest all-electric vehicle technology.

While the 2024 Chevy Blazer EV will be available to civilians in a wide variety of configurations and trim levels, Chevy will also offer a Police Pursuit Vehicle (PPV) variant to law enforcement. Now, we're getting a thorough look at what the new 2024 Chevy Blazer EV PPV has to offer thanks to a recently released video.

Clocking in at 12 minutes and 26 seconds, the video provides an overview of all the features of the first pursuit-rated EV based on the GM Ultium platform. Highlights of the 2024 Chevy Blazer EV PPV include a 400-volt all-wheel-drive propulsion system. Maximum output is set at 498 horsepower and 531 pound-feet of torque. There's also an even 50/50 front-to-rear weight distribution for enhanced handling, while the onboard 105 kWh battery provides an estimated 250 miles of range on a full charge.

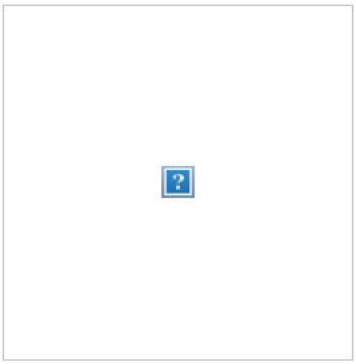
Upgraded heavy duty suspension and six-piston Brembo front brake calipers (matched to 15.3-inch rotors) help to handle the heft, while a set of underbody

skid plates protect the bits under the body. The police crossover also rides on 20-inch steel wheels wrapped in Firestone Firehawk Pursuit tires.

Click for Full Story

ADVERTORIAL | Stalker Radar

The LidarCam 2: Where Cutting-Edge Lidar Speed Enforcement Meets Undeniable Photo and Video Evidence Capture



Automatically collect a video + multiple high-resolution photos every time you capture a traffic violation. Built-in License Plate Reading Technology (ANPR/ALPR) can automatically check for wanted plates or other violations. Hand-held or mounted to a tripod, the Stalker LidarCam 2 is the next generation of photo enforcement.

Up to 1TB of internal storage allows you to save multiple days-worth of evidence onboard before you upload them into the included secure PC-based Evidence Manager software for viewing, processing, and sharing. AES-256 encryption comes standard, keeping your data secure.

The LidarCam 2 is equipped with built-in GPS, USB-C, and Wi-Fi, with optional 4G-LTE cellular connection available. Fully-remote wireless operation in real time on any platform - phone, tablet, or desktop - with no proprietary apps needed. Learn more at StalkerRadar.com/video-lidar or call us today at 1-800-STALKER.

PRODUCTS

Underseat Storage System From Pro-gard Products



Pro-gard Products LLC introduces the Under Seat Storage System for F-150 and Super Duty Crew Cabs, catering to law enforcement storage needs.

This advanced solution optimizes cargo space for equipment and weapons while ensuring secure, organized storage. Its dual compartments offer versatility with a removable divider and locking latches for weapon security. Constructed from durable steel with a textured black powder coat finish, it includes a rubber mat-lined floor for protection. Installation is effortless, attaching seamlessly to OEM holes without drilling.

Pro-gard's commitment to enhancing officer efficiency and safety shines throughout this innovative system.

Click for Pro-gard Products

Do you have news to share?

Please contact National Director, Kirk Moen: kmoen@signalbusinessgroup.com for more information.

Signal Business Group LLC
PO Box 3157, Bluffton, SC 29910-3157
P: 224-458-1123
E: info@signalbusinessgroup.com

Visit Us | 2023 Media Kit | See you in Forth Worth, TX 2024!

If you wish to unsubscribe from our newsletter, click here

From: Police Fleet Professional Magazine
To: Robles, Francis Jr. (POL)
Subject: September 2023 eNews End of Month
Date: Friday, September 29, 2023 5:15:14 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.

Logo

Sponsored by General Tire & Tufloc

INDUSTRY NEWS

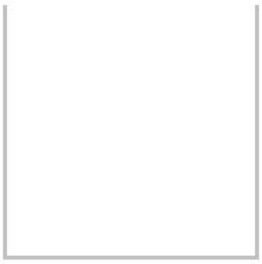
Sartell Adds Military Themed Squad Car to the Fleet

The Sartell Police Department (MN) unveiled a new, military service-themed squad car that will be used by police officers who are also military veterans.

The eye-catching design helps bring attention to the local organizations working with veterans fighting PTSD and working to prevent soldier and first responder suicide.

The emblems of the Invisible Wounds Project, Soldier's 6, and 23rd Veteran programs are prominently displayed on the squad car.

Sartell Police Chief Brandon Silgjord says he's honored to have the vehicle on active patrol and hopes it's a symbol to the community that no one fights alone.





Click for Full Story

Claremont PD Rolls Out New Electric Cruiser



The Claremont Police Department (NH) is showing off some new digs.

The department now has a fully electric F150 pickup truck in it's fleet, donated by the local dealership Ford of Claremont.

The department says it is the first municipality in the Northeast to use this type of vehicle on patrol. The Chief says it's a positive change for the department.

"You know we haven't had to put gas in the car so we have saved money right there. Right out of the gate. So, it is interesting, it is definitely something that we are getting used to," Chief Brent Wilmot said. "I think it is something that this profession, law enforcement in general will be getting used to in the coming years."

Ford of Claremont also donated a charging station and emergency lights. This is the second vehicle the business has donated to the department in recent years.

Click for Full Story

GM Presents In-Depth Overview Of 2024 Chevy Blazer EV Police Pursuit Vehicle



The 2024 Chevy Blazer EV was unveiled in July of 2022, with GM pulling the sheets on a new midsize crossover propelled by The General's latest all-electric vehicle technology.

While the 2024 Chevy Blazer EV will be available to civilians in a wide variety of configurations and trim levels, Chevy will also offer a Police Pursuit Vehicle (PPV) variant to law enforcement. Now, we're getting a thorough look at what the new 2024 Chevy Blazer EV PPV has to offer thanks to a recently released video.

Clocking in at 12 minutes and 26 seconds, the video provides an overview of all the features of the first pursuit-rated EV based on the GM Ultium platform. Highlights of the 2024 Chevy Blazer EV PPV include a 400-volt all-wheel-drive propulsion system. Maximum output is set at 498 horsepower and 531 pound-feet of torque. There's also an even 50/50 front-to-rear weight distribution for enhanced handling, while the onboard 105 kWh battery provides an estimated 250 miles of range on a full charge.

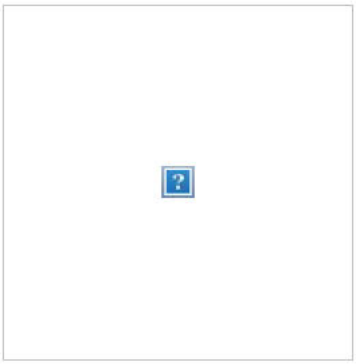
Upgraded heavy duty suspension and six-piston Brembo front brake calipers (matched to 15.3-inch rotors) help to handle the heft, while a set of underbody

skid plates protect the bits under the body. The police crossover also rides on 20-inch steel wheels wrapped in Firestone Firehawk Pursuit tires.

Click for Full Story

ADVERTORIAL | Stalker Radar

The LidarCam 2: Where Cutting-Edge Lidar Speed Enforcement Meets Undeniable Photo and Video Evidence Capture



Automatically collect a video + multiple high-resolution photos every time you capture a traffic violation. Built-in License Plate Reading Technology (ANPR/ALPR) can automatically check for wanted plates or other violations. Hand-held or mounted to a tripod, the Stalker LidarCam 2 is the next generation of photo enforcement.

Up to 1TB of internal storage allows you to save multiple days-worth of evidence onboard before you upload them into the included secure PC-based Evidence Manager software for viewing, processing, and sharing. AES-256 encryption comes standard, keeping your data secure.

The LidarCam 2 is equipped with built-in GPS, USB-C, and Wi-Fi, with optional 4G-LTE cellular connection available. Fully-remote wireless operation in real time on any platform - phone, tablet, or desktop - with no proprietary apps needed. Learn more at StalkerRadar.com/video-lidar or call us today at 1-800-STALKER.

PRODUCTS

Underseat Storage System From Pro-gard Products



Pro-gard Products LLC introduces the Under Seat Storage System for F-150 and Super Duty Crew Cabs, catering to law enforcement storage needs.

This advanced solution optimizes cargo space for equipment and weapons while ensuring secure, organized storage. Its dual compartments offer versatility with a removable divider and locking latches for weapon security. Constructed from durable steel with a textured black powder coat finish, it includes a rubber mat-lined floor for protection. Installation is effortless, attaching seamlessly to OEM holes without drilling.

Pro-gard's commitment to enhancing officer efficiency and safety shines throughout this innovative system.

Click for Pro-gard Products

Do you have news to share?

Please contact National Director, Kirk Moen: kmoen@signalbusinessgroup.com for more information.

Signal Business Group LLC
PO Box 3157, Bluffton, SC 29910-3157
P: 224-458-1123
E: info@signalbusinessgroup.com

Visit Us | 2023 Media Kit | See you in Forth Worth, TX 2024!

If you wish to unsubscribe from our newsletter, click here

From: Police Fleet Professional Magazine
To: Flaherty, Kevin J (POL)
Subject: September 2023 eNews End of Month
Date: Friday, September 29, 2023 5:30:25 PM

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

Logo

Sponsored by General Tire & Tufloc

INDUSTRY NEWS

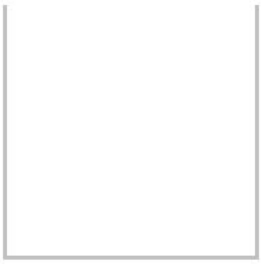
Sartell Adds Military Themed Squad Car to the Fleet

The Sartell Police Department (MN) unveiled a new, military service-themed squad car that will be used by police officers who are also military veterans.

The eye-catching design helps bring attention to the local organizations working with veterans fighting PTSD and working to prevent soldier and first responder suicide.

The emblems of the Invisible Wounds Project, Soldier's 6, and 23rd Veteran programs are prominently displayed on the squad car.

Sartell Police Chief Brandon Silgjord says he's honored to have the vehicle on active patrol and hopes it's a symbol to the community that no one fights alone.





Click for Full Story

Claremont PD Rolls Out New Electric Cruiser



The Claremont Police Department (NH) is showing off some new digs.

The department now has a fully electric F150 pickup truck in it's fleet, donated by the local dealership Ford of Claremont.

The department says it is the first municipality in the Northeast to use this type of vehicle on patrol. The Chief says it's a positive change for the department.

"You know we haven't had to put gas in the car so we have saved money right there. Right out of the gate. So, it is interesting, it is definitely something that we are getting used to," Chief Brent Wilmot said. "I think it is something that this profession, law enforcement in general will be getting used to in the coming years."

Ford of Claremont also donated a charging station and emergency lights. This is the second vehicle the business has donated to the department in recent years.

Click for Full Story

GM Presents In-Depth Overview Of 2024 Chevy Blazer EV Police Pursuit Vehicle



The 2024 Chevy Blazer EV was unveiled in July of 2022, with GM pulling the sheets on a new midsize crossover propelled by The General's latest all-electric vehicle technology.

While the 2024 Chevy Blazer EV will be available to civilians in a wide variety of configurations and trim levels, Chevy will also offer a Police Pursuit Vehicle (PPV) variant to law enforcement. Now, we're getting a thorough look at what the new 2024 Chevy Blazer EV PPV has to offer thanks to a recently released video.

Clocking in at 12 minutes and 26 seconds, the video provides an overview of all the features of the first pursuit-rated EV based on the GM Ultium platform. Highlights of the 2024 Chevy Blazer EV PPV include a 400-volt all-wheel-drive propulsion system. Maximum output is set at 498 horsepower and 531 pound-feet of torque. There's also an even 50/50 front-to-rear weight distribution for enhanced handling, while the onboard 105 kWh battery provides an estimated 250 miles of range on a full charge.

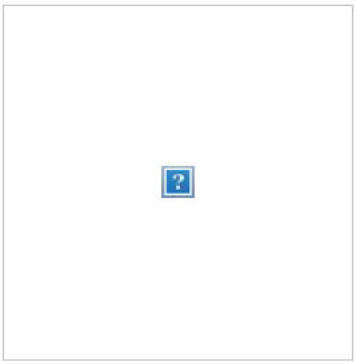
Upgraded heavy duty suspension and six-piston Brembo front brake calipers (matched to 15.3-inch rotors) help to handle the heft, while a set of underbody

skid plates protect the bits under the body. The police crossover also rides on 20-inch steel wheels wrapped in Firestone Firehawk Pursuit tires.

Click for Full Story

ADVERTORIAL | Stalker Radar

The LidarCam 2: Where Cutting-Edge Lidar Speed Enforcement Meets Undeniable Photo and Video Evidence Capture



Automatically collect a video + multiple high-resolution photos every time you capture a traffic violation. Built-in License Plate Reading Technology (ANPR/ALPR) can automatically check for wanted plates or other violations. Hand-held or mounted to a tripod, the Stalker LidarCam 2 is the next generation of photo enforcement.

Up to 1TB of internal storage allows you to save multiple days-worth of evidence onboard before you upload them into the included secure PC-based Evidence Manager software for viewing, processing, and sharing. AES-256 encryption comes standard, keeping your data secure.

The LidarCam 2 is equipped with built-in GPS, USB-C, and Wi-Fi, with optional 4G-LTE cellular connection available. Fully-remote wireless operation in real time on any platform - phone, tablet, or desktop - with no proprietary apps needed. Learn more at StalkerRadar.com/video-lidar or call us today at 1-800-STALKER.

PRODUCTS

Underseat Storage System From Pro-gard Products



Pro-gard Products LLC introduces the Under Seat Storage System for F-150 and Super Duty Crew Cabs, catering to law enforcement storage needs.
This advanced solution optimizes cargo space for equipment and weapons while ensuring secure, organized storage. Its dual compartments offer versatility with a removable divider and locking latches for weapon security. Constructed from durable steel with a textured black powder coat finish, it includes a rubber mat-lined floor for protection. Installation is effortless, attaching seamlessly to OEM holes without drilling.
Pro-gard's commitment to enhancing officer efficiency and safety shines throughout this innovative system.

Click for Pro-gard Products

Do you have news to share?

Please contact National Director, Kirk Moen: kmoen@signalbusinessgroup.com for more information.

Signal Business Group LLC
PO Box 3157, Bluffton, SC 29910-3157
P: 224-458-1123
E: info@signalbusinessgroup.com

Visit Us | 2023 Media Kit | See you in Forth Worth, TX 2024!

If you wish to unsubscribe from our newsletter, click here

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Slain LEO"s family wants judge to resign; NOPD"s Mardi Gras staffing woes
Date: Monday, January 9, 2023 2:28:34 PM

January 9, 2023 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Today is National Law Enforcement Appreciation Day (L.E.A.D.), established in 2014 by the Concerns of Police Survivors (C.O.P.S.) to encourage everyone to show support for the more than 800,000 law enforcement officers in America. Learn more here.

In honor of your courage and commitment to protect and serve our communities, today sees the launch of Police1's "50 states, 50 police heroes," our annual roundup of how law enforcement stepped up through acts of heroism to create some good this past year.

From an Alabama cop whose uniform melted off his body as he rescued a 3-year-old from a fire to the Wyoming LEOs who 'beefed up' patrol ahead of a holiday weekend to steer cattle away from oncoming traffic, click here to read about the amazing acts of bravery and kindness (with some fun moments too) that our nation's LEOs demonstrate every day.

Stay safe,

— The Police1 Team

TOP STORIES

Family of slain Calif. deputy calls for judge to resign

Colleagues, friends and family members have questioned why the suspect wasn't behind bars under the state's "three strikes" law

New Orleans' depleted police force brings unique challenges during Mardi Gras

'We need more cops': Philly PD sending more officers to city's most violent areas

'Thankful to still be alive': N.C. deputy shot during struggle with suspect continues to recover

Wash. county struggles to find funds to cover $19.5M in damages to former deputy, wife

'Aggressive deputy' who pulled over multiple drivers exposed as 19-year-old impersonator

Nominations are open for 2023 Axon Rise Awards!

RISE Awards are designed to highlight the heroism of public safety professionals who go beyond the call of duty. Nominations are open through January 20 and voting opens January 23rd!

Nominate a Hero Today!

OFFICER WELLNESS

How police leaders can set officers on a pathway to resilience

By Sergeant Steven Breakall and Sergeant Eric Thornton

Download a resiliency checklist to measure the four most effective pathways to resilience: hardiness, self-enhancement, repressive coping and positive emotions

Why building trust is critical to building an effective officer wellness program

By James Careless

The process of building trust begins with buy-in by everyone in the department

Help is just one call away



By Christopher Littrell
How a retired police commander is changing the narrative of mental health and healing

NATIONAL LAW ENFORCEMENT APPRECIATION DAY



50 states, 50 police heroes: Honoring our LEOs on National Law Enforcement Appreciation Day

By Police1 Staff
See how law enforcement stepped up through acts of heroism to create some good this past year



Beyond 'Thank you for your service': How to encourage citizen support of law enforcement officers

By Chief Joel F. Shults, Ed.D.
Nurturing positive community relationships is an integral part of maintaining a positive trajectory for police morale, enthusiasm and commitment



SPONSORED CONTENT



New ALPR system puts dent in Ohio city's crime

In Bowling Green an advanced new system provides not just still images but reviewable video and advanced analysis of passing vehicles – and that's helping solve a lot of cases.

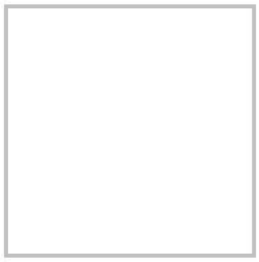


FEATURED RESOURCES

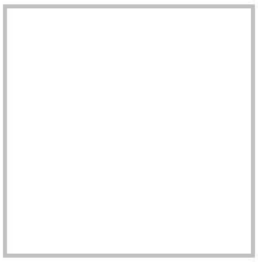
How to Buy Police Drones
Download to learn key steps for product selection,

FEATURED RESOURCES

How to Buy Investigation Software (eBook)
Download to learn key steps



purchasing and implementation.



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: info@lahidtatraining.org
To: Burton, Ray (POL)
Subject: Some Upcoming In-Person and Live-Stream Training
Date: Wednesday, July 26, 2023 1:52:36 PM

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



Below are several classes that are listed on the LA HIDTA Training website at www.lahidtatraining.org. If you have any questions or need any assistance with anything regarding training, do not hesitate to email me at Kenneth.Cordray@laclear.ca.gov.

This is only a small portion of classes listed on the training website. Don't forget to also search by "Tags" to search by county, free, online, Armorer school, CNOA, JRIC, POST Certified, STC Certified, Electronic Surveillance or Watch Center Orientation. Also, you can click the "Next" button to take you to the next two months of the training calendar.

August 01, 2023 - Tuesday
LA CLEAR Overview & Watch Center Orientation
Commerce, CA
Click to Register
Download Flyer

Free Class - A must for ANY Investigator

Law Enforcement Personnel Only

August 28, 2023 - Monday
Assault Weapon Identification & New and Upcoming CA Gun Laws
Commerce, CA
Click to Register
Download Flyer

POST Certified - Plan IV

Free In-Person Class - No Walk-ins will be allowed in the Class

August 30, 2023 - Wednesday
Mental Health & Firearms
Commerce, CA
Download Flyer

Click to Register

September 06, 2023 - Wednesday
Snapchat Investigations
Commerce, CA
Download Flyer

Click to Register

August 01, 2023 - Tuesday
License Plate Recognition Technology: Basic User
Santa Monica, CA
Download Flyer

Free Class - POST Certified

Apply for Training

August 01, 2023 - Tuesday
Image Comparison Technology: Basic User
Santa Monica, CA
Download Flyer

Free Class

Apply for Training

August 02, 2023 - Wednesday
Google for Law Enforcement
Commerce, CA
Download Flyer

Click to Register

August 02, 2023 - Wednesday
Policing Violent Extremism I - ISIS/ISIL and the Evolution of Al Qaeda
Rancho Cucamonga, CA
Download Flyer

POST & STC Certified

Free Class

Apply for Training

August 02-30, 2023; Wednesday - Wednesday
Communications Training Officer Certification Course
Download Flyer

POST Certified

Live-Stream - 0800-1700 Hrs PST

5 Sessions - Every Wednesday

Click to Apply

August 03, 2023 - Thursday
Drug Related Conspiracy Investigations: The Investigative Process Through Case Study
Commerce, CA
Click to Register
Download Flyer

Free Class

Restricted to L.E./Military/Fire Personnel

August 03, 2023 - Thursday
Electronic Surveillance
San Rafael, CA
Download Flyer

Click to Register

POST Certified - Free for POST Reimbursable Agencies

August 03, 2023 - Thursday
FTO Update: Module I
Download Flyer

Live-Stream Course - 0800-1700 Hrs PST

POST & STC Certified

Click to Register

August 03, 2023 - Thursday
Combat Handgun for Law Enforcement Women
Corona, CA
Download Flyer

POST Certified - Plan IV

Apply for Training

August 03, 2023 - Thursday
Child Abuse: From Suspicion To Disclosure
Download Flyer

Free Webinar - 0800-1500 Hrs PST

Click for Information and Registration

August 04, 2023 - Friday
"Close Quarters" Combat for LE Women
Corona, CA
Download Flyer

Apply for Training

August 07, 2023 - Monday
The Patrol Search Warrant
Commerce, CA
Download Flyer

POST Certified

Click to Register

August 08, 2023 - Tuesday
Cyber Warrior Academy
Paso Robles, CA
Download Flyer

POST Certified

Free Class - Restricted to L.E. Personnel

Apply for Training

August 09, 2023 - Wednesday
CI's and Search Warrants

Free Webinar 1800-1930 Hrs PST

Click for Details and Registration

August 09, 2023 - Wednesday
Automated License Plate Reader (ALPR) - Technology and Procedures
Danville, CA

Free Class - POST Certified

Click for Information and Apply for Training

August 09-10, 2023; Wednesday - Thursday
Human Trafficking
Free Webinar - 0800-1600 Hrs PST

Click for Information and Registration

August 10, 2023 - Thursday
School Safety Seminar
Azusa, CA

Download Flyer

Free Seminar

Apply for Training

August 14, 2023 - Monday
PC 290 Sex Offender Tracking & Registration Enforcement
Commerce, CA
Download Flyer

POST Certified

Apply for Training

August 14, 2023 - Monday
Tactical Emergency Casualty Care for Law Enforcement & First Responders Course
Rohnert Park, CA
Download Flyer

POST & NAEMT Certified

Click to Register

August 14-15, 2023; Monday - Tuesday
SWAT Tactics & Update Course
Arcadia, CA
Download Flyer

POST Certified

See Flyer for Registration

August 15, 2023 - Tuesday
Fundamentals of Gang Recognition

Download Flyer

STC Certified

Live-Stream - 0800-1600 Hrs PST

Click to Register

August 15-16, 2023; Tuesday - Wednesday
Tactical Emergency Casualty Care (TECC)
San Diego, CA
Download Flyer

NAEMT Certified

UASI Reimbursable

Click to Register

August 16-18, 2023; Wednesday - Friday
NIST UAS Train the Trainer
Fountain Valley, CA
Download Flyer

Apply for Training

August 17, 2023 - Thursday
Unlocking Digital Clues: Enhancing Investigations through Social Media Intelligence

Free Webinar - 1100-1200 Hrs PST

Click for Information & Registration

August 18, 2023 - Friday
Cultural Diversity

Ontario, CA
Download Flyer
POST & STC Certified

Click to Apply

August 19, 2023 - Saturday
Conflict Management
Download Flyer
POST Certified

Live-Stream - 0800-1200 Hrs PST

Click to Apply

August 19-22, 2023; Saturday - Tuesday
Communications Training Officer Certification Course
Download Flyer

POST Certified

Live-Stream - 0800-1700 Hrs PST

Click to Apply

August 21, 2023 - Monday
Tactical Emergency Casualty Care for Law Enforcement & First Responders Course
Commerce, CA
Download Flyer

POST & NAEMT Certified

Click to Register

August 21, 2023 - Monday

Asset/Crypto Seizure and Forfeiture
Paso Robles, CA
Download Flyer

POST Certified

Apply for Training

August 22, 2023 - Tuesday
Combatting Human Trafficking
Diamond Bar, CA
Download Flyer

Free Class - See In-Person or Live-Stream - 0800-1200 Hrs PST

Apply for Training - In-Person

Apply for Training - Live-Stream

August 22, 2023 - Tuesday
Terrorism Liaison Officer (TLO) Basic Course
Santa Rosa, CA

Free Class - Limited to NCRIC AOR

Click for Information and Apply for Training

August 22, 2023 - Tuesday
Child Sex Trafficking: From Suspicion To Disclosure
Download Flyer

Free Webinar - 0700-1400 Hrs PST

Click for Information and Registration

August 22-23, 2023; Tuesday - Wednesday

Ballistic Shield Operator Course
San Francisco, CA
Download Flyer

Click to Register

August 22-23, 2023; Tuesday - Wednesday
i2 Analyst Notebook Advanced
Free Live-Stream - 0800-1700 Hrs PST

Click for Information & Registration

August 23, 2023 - Wednesday
Policing Violent Extremism I
Dublin, CA

Free Class

Click for Information and Apply for Training

August 24, 2023 - Thursday
Dispatch, Stress Management for Supervisors or Managers
Download Flyer

POST Certified

Live-Stream - 0800-1200 Hrs PST

Click to Apply

August 24, 2023 - Thursday
Crisis Intervention & De-Escalation Training
Download Flyer

Live-Stream Course - 0800-1700 Hrs PST

POST Certified - Free for POST-Reimbursable Agencies

Click to Register

August 25, 2023 - Friday
Tactical Emergency Casualty Care for Law Enforcement & First Responders Course
Los Angeles, CA
Download Flyer

POST & NAEMT Certified

Click to Register

August 28, 2023 - Monday
Fentanyl Overdose Investigations
Dublin, CA
Download Flyer

Apply for Training

August 28-29, 2023; Monday - Tuesday
Leadership & Accountability: Leading with Influence
Mountain View, CA
Download Flyer

POST & STC Certified

Click to Register

August 28-29, 2023; Monday - Tuesday
Two-Day Basic Peer Support Training
Santa Ana, CA
Download Flyer

POST & STC Certified

Click to Register

August 29, 2023 - Tuesday
Record of Arrest and Prosecution (RAP) Sheet Training
Download Flyer

Free Live-Stream - 0830-1200 Hrs

POST & STC Certified

Click to Register

August 30, 2023 - Wednesday
Hot & Fresh Pursuit

Free Webinar 1600-1730 Hrs PST

Click for Details and Registration

August 30-31, 2023; Wednesday - Thursday
AR15/M4 (Unbranded) Armorer Course
San Bernardino, CA
Download Flyer

Click to Register

August 30-September 01, 2023; Wednesday - Friday
Leadership Training: Assertive Supervision - Practical Approaches to Performance Management
Mountain View, CA
Download Flyer

POST & STC Certified

Click to Register

August 31, 2023 - Thursday
Organized Crime: The Mexican Mafia
Commerce, CA
Download Flyer

Click to Register

August 31, 2023 - Thursday
The Anatomy of a Criminal Vehicle - Hidden Compartment Training
San Diego, Ca
Download Flyer

Apply For Training

August 31-September 01, 2023; Thursday - Friday
Mantracking Tactics 2-Day Course
San Bernardino, CA
Download Flyer

Click for Information & Registration

September 01, 2023 - Friday
Electronic Surveillance (Wiretap)
Monterey, CA
Download Flyer

POST Certified – Free for Local POST Agencies

Click to Register

September 05, 2023 - Tuesday
Assault Weapon Identification & New and Upcoming CA Gun Laws
Commerce, CA
Click to Register

Download Flyer

POST Certified - Plan IV

Free In-Person Class - No Walk-ins will be allowed in the Class

September 05-07, 2023; Tuesday - Thursday
Advanced Interview & Interrogation
Newport Beach, CA
Download Flyer

POST Certified

Apply for Training

September 06, 2023 - Wednesday
Airport & Border Searches

Free Webinar 1300-1400 Hrs PST

Click for Details and Registration

September 07, 2023 - Thursday
Overdose Death (OD) Investigations
Irvine, CA
Download Flyer

Apply for Training

September 07-08, 2023; Thursday - Friday
Advanced Search Warrants
Commerce, CA
Download Flyer

Click to Register

September 11-13, 2023; Monday - Wednesday
Understanding sUAS Maintenance
San Bernardino, CA
Download Flyer

Click to Register

September 12, 2023 - Tuesday
Electronic Surveillance (Wiretap)
Commerce, CA
Download Flyer

Click to Register

POST Certified – Free for Local POST Agencies

September 12, 2023 - Tuesday
Targeted Violence Prevention
Corona, CA
Download Flyer

POST Certified

Free Class

Apply for Training

September 12-13, 2023; Tuesday - Wednesday
SWAT Tactics & Update Course
Castaic, CA
Download Flyer

POST Certified

See Flyer for Registration

September 19, 2023 - Tuesday
Drugged Driving Investigations & Drug Abuse Recognition (DAR)
Simi Valley, CA
Download Flyer

POST & STC Certified

Click to Register

September 25-26, 2023; Monday - Tuesday
Social Media and OSINT
Burbank, CA
Download Flyer

Click to Register

September 27-29, 2023; Wednesday - Friday
3-Day Sex Offender Supervision Officer (SOSO) Summit
Lake Tahoe, CA

POST and STC Certified
Click to Register

September 29, 2023 - Friday
Civilian Leadership Course for Public Safety Personnel
Paso Robles, CA
Download Flyer

Apply for Training

October 02-03, 2023; Monday - Tuesday
870 Remington Shotgun Armorer Course
Bakersfield, CA
Download Flyer

RemArms Authorized Armorer School

Click to Register

October 17-20, 2023; Tuesday - Friday
Tactical Rifle Instructor Course
Chino, CA
Download Flyer

POST Certified

Click to Register

October 23-November 03, 2023; Monday - Friday
Special Weapons & Tactics Course
Carlsbad, CA
Download Flyer

POST Certified

See Flyer for Registration

www.lahidtatraining.org for Training Calendar

info@lahidtatraining.org for info/questions

Kenneth.Cordray@laclear.ca.gov for Trainers and Schedule New Classes

https://instruq.co for our online training partner

To remove yourself from this mailing list, Click here

From: IACP
To: Powers, Liam (POL)
Subject: State & Provincial Police Planning Officers Section SPPPOS Digest for Wednesday February 22, 2023
Date: Thursday, February 23, 2023 12:18:25 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.

State & Provincial Police Planning Officers Section SPPPOS

Post New Message

Feb 22, 2023

Discussions

started 8 hours ago, Keitha Pritchard (0 replies)

EVOC and TIMs

1. Good afternoon, New Mexico State Police is... Keitha Pritchard

started 11 hours ago, Emily Perkins (4 replies)

Wrong-way pursuits

Good afternoon all: The Kentucky State... Emily Perkins
Good afternoon, The Vermont State Police... Timothy Gould
Wonderful, thank you so much! Emily M.... Emily Perkins
Hey Emily, Our policy states the below... Sarah Hurst
Afternoon, Our policy does not list wrong... Edward Larney

started 12 hours ago, Brina Gendhar (0 replies)

Civilians working in Crime Prevention

7. Good afternoon, The Michigan State... Brina Gendhar

started 16 days ago, Andrew Hyer (5 replies)

ALPR Policy/Guidance

Afternoon, we do not have carry them on patrol... Edward Larney
Lt Hyer, Please see the below responses... Sarah Hurst

started 2 months ago, Angela Killion (3 replies)

Employee training records/histories

10. At DSP, we print out their certificate or... Edward Larney

top next

1. EVOC and TIMs

Reply to Group | Reply to Sender

Feb 22, 2023 3:55 PM
Keitha Pritchard

Good afternoon,

New Mexico State Police is requesting information from other agencies for EVOC and TIMs programs.

More specifically, does your agency have full-time or part-time EVOC and TIMs units/instructors? If you have a full-time unit how many are on it and how is it structured? If your agency has part-time instructors, how is your agency conducting the instruction (i.e. frequency of instruction to department personnel, requirements for instructors)?

Do you have any policies or directives for this?

Thank you,

KC Pritchard

New Mexico State Police

Keitha Pritchard
Officer
New Mexico State Police
NM

Reply to Group Online View Thread Recommend Forward

Flag as Inappropriate

2. Wrong-way pursuits

Reply to Group | Reply to Sender

Feb 22, 2023 12:58 PM
Emily Perkins

Good afternoon all:

The Kentucky State Police seem to be encountering more instances of becoming involved in pursuits traveling in the wrong direction on divided highways. We are hoping to obtain a copy of any policies, training materials, guidelines, legal decisions, or other information your agency may have specific to wrong-way driver pursuits. Please feel free to reply here or by email to emilym.perkins@ky.gov.

Thank you so much for your assistance with this topic.

Emily M. Perkins
Procedures Development Specialist
Strategic Planning Branch
Kentucky State Police
emilym.perkins@ky.gov

Reply to Group Online **View Thread** **Recommend** **Forward**

Flag as Inappropriate

3. Re: Wrong-way pursuits

Reply to Group | Reply to Sender

Feb 22, 2023 1:07 PM | view attached

Timothy Gould

Good afternoon,

The Vermont State Police strictly prohibit our Troopers from pursuing in a wrong way direction. Our pursuit intervention tactics policy has separate standards than engaging in a pursuit, so Troopers can still deploy intervention tactics if the circumstances warrant.

I have attached a copy of each policy.

Thank you,

Lt. Tim Gould
Professional Standards
Vermont State Police

Reply to Group Online View Thread Recommend Forward
Flag as Inappropriate

Original Message:
Sent: 2/22/2023 12:58:00 PM
From: Emily Perkins
Subject: Wrong-way pursuits

Good afternoon all:

The Kentucky State Police seem to be encountering more instances of becoming involved in pursuits traveling in the wrong direction on divided highways. We are hoping to obtain a copy of any policies, training materials, guidelines, legal decisions, or other information your agency may have specific to wrong-way driver pursuits. Please feel free to reply here or by email to emilym.perkins@ky.gov.

Thank you so much for your assistance with this topic.

Emily M. Perkins
Procedures Development Specialist
Strategic Planning Branch
Kentucky State Police
emilym.perkins@ky.gov
---

4. Re: Wrong-way pursuits

Reply to Group | Reply to Sender

Feb 22, 2023 1:09 PM
Emily Perkins

Wonderful, thank you so much!

Emily M. Perkins
Strategic Planning Branch
Kentucky State Police

Reply to Group Online **View Thread** **Recommend** **Forward**

Flag as Inappropriate

Original Message:
Sent: 2/22/2023 12:58:00 PM
From: Emily Perkins
Subject: Wrong-way pursuits

Good afternoon all:

The Kentucky State Police seem to be encountering more instances of becoming involved in pursuits traveling in the wrong direction on divided highways. We are hoping to obtain a copy of any policies, training materials, guidelines, legal decisions, or other information your agency may have specific to wrong-way driver pursuits. Please feel free to reply here or by email to emilym.perkins@ky.gov.

Thank you so much for your assistance with this topic.

Emily M. Perkins
Procedures Development Specialist
Strategic Planning Branch

Kentucky State Police
emilym.perkins@ky.gov
---

top previous next

5. Re: Wrong-way pursuits

Reply to Group Reply to Sender

Feb 22, 2023 3:12 PM | view attached

Sarah Hurst

Hey Emily,

Our policy states the below language for wrong way pursuits. I have attached the entire policy as well. The below is on Page 9.

C. Patrol vehicles **shall only be used** for the purposes listed below **as a last resort and when deadly force is justified.**

The determination to use a patrol vehicle for the purposes listed below is the sole decision of the pursuing Member.

1. Pursuing a vehicle in a direction opposite to the flow of traffic on a divided highway, and
2. Ramming or forcing the suspect's vehicle off the roadway

Sarah Hurst | Sergeant
Research, Planning and Development
1150 Foster Avenue
Nashville, TN 37243
p. 615-854-6814
sarah.hurst@tn.gov
tn.gov/safety

Reply to Group Online View Thread Recommend Forward

Flag as Inappropriate

Original Message:
Sent: 2/22/2023 12:58:00 PM
From: Emily Perkins
Subject: Wrong-way pursuits

Good afternoon all:

The Kentucky State Police seem to be encountering more instances of becoming involved in pursuits traveling in the wrong direction on divided highways. We are hoping to obtain a copy of any policies, training materials, guidelines, legal decisions, or other information your agency may have specific to wrong-way driver pursuits. Please feel free to reply here or by email to emilym.perkins@ky.gov.

Thank you so much for your assistance with this topic.

Emily M. Perkins
Procedures Development Specialist
Strategic Planning Branch
Kentucky State Police
emilym.perkins@ky.gov
---

top previous next

6. Re: Wrong-way pursuits

Reply to Group Reply to Sender

Feb 22, 2023 3:28 PM | view attached

Edward Larney

Afternoon,

Our policy does not list wrong way pursuits as an automatic disqualifier technically,

however, based upon our guidelines, it would likely be terminated. I have attached our pursuit policy.

Edward Larney
Sergeant
Delaware State Police
DE

Reply to Group Online **View Thread** **Recommend** **Forward**

Flag as Inappropriate

Original Message:
Sent: 02-22-2023 12:57
From: Emily Perkins
Subject: Wrong-way pursuits

Good afternoon all:

The Kentucky State Police seem to be encountering more instances of becoming involved in pursuits traveling in the wrong direction on divided highways. We are hoping to obtain a copy of any policies, training materials, guidelines, legal decisions, or other information your agency may have specific to wrong-way driver pursuits. Please feel free to reply here or by email to emilym.perkins@ky.gov.

Thank you so much for your assistance with this topic.

Emily M. Perkins
Procedures Development Specialist
Strategic Planning Branch
Kentucky State Police
emilym.perkins@ky.gov

Reply to Group | Reply to Sender

Feb 22, 2023 11:47 AM
Brina Gendhar

Good afternoon,

The Michigan State Police is inquiring to see if any agencies use civilian members to complete crime prevention activities, for crime prevention purposes, and/or crime prevention related positions?

All responses may be directed to F/Lt. Brian McComb at MccombB1@michigan.gov

Thank you!

Brina

Brina Gendhar
Planning, Research, and Accreditation Section
Michigan State Police
Lansing, Michigan
517-719-4613
gendharb@michigan.gov

Reply to Group Online | View Thread | Recommend | Forward
Flag as Inappropriate

top previous next

8. Re: ALPR Policy/Guidance

Reply to Group | Reply to Sender

Feb 22, 2023 3:18 PM | view attached

Edward Larney

Afternoon, we do not have carry them on patrol vehicles, just at stationary locations. I have included our policy on these.

Edward Larney
Sergeant
Delaware State Police
DE

Reply to Group Online View Thread Recommend Forward

Flag as Inappropriate

Original Message:
Sent: 02-06-2023 18:35
From: Andrew Hyer
Subject: ALPR Policy/Guidance

The Wisconsin State Patrol is going to be activating the ALPR feature on our Fleet 3 cameras and is looking for information about the use of ALPR.

1. Does your agency use LPR/ALPR technology in squad cars?
2. What policies have been established for how the technology is used? Please share any policies or operating procedures.
3. How long is data from the system retained under your retention policy?

Thank you for the information in advance.

Andrew Hyer
Lieutenant
Special Operation Section
Wisconsin State Patrol
andrew.hyer@dot.wi.gov
(608) 316-0857
---

top previous next

9. Re: ALPR Policy/Guidance

Reply to Group | Reply to Sender

Feb 22, 2023 3:29 PM | view attached

Sarah Hurst

Lt Hyer,

Please see the below responses from the Tennessee Highway Patrol.

1. Does your agency use LPR/ALPR technology in squad cars? Yes, some – We have 64 vehicles with LPR's
2. What policies have been established for how the technology is used? Please share any policies or operating procedures. Attached.
3. How long is data from the system retained under your retention policy? 90 Days

If you need any additional information please let me know.

Thanks,

Sarah Hurst |Sergeant
Research, Planning and Development
1150 Foster Avenue
Nashville, TN 37243
p. 615-854-6814
sarah.hurst@tn.gov
tn.gov/safety

Original Message:

Sent: 2/6/2023 6:35:00 PM
From: Andrew Hyer
Subject: ALPR Policy/Guidance

The Wisconsin State Patrol is going to be activating the ALPR feature on our Fleet 3 cameras and is looking for information about the use of ALPR.

1. Does your agency use LPR/ALPR technology in squad cars?
2. What policies have been established for how the technology is used? Please share any policies or operating procedures.
3. How long is data from the system retained under your retention policy?

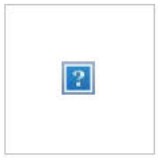
Thank you for the information in advance.

Andrew Hyer
Lieutenant
Special Operation Section
Wisconsin State Patrol
andrew.hyer@dot.wi.gov
(608) 316-0857
---

top previous

10. Re: Employee training records/histories

Reply to Group Reply to Sender



Feb 22, 2023 3:11 PM
Edward Larney

At DSP, we print out their certificate or training record and physically add it their personnel file.

Edward Larney
Sergeant
Delaware State Police
DE

Reply to Group Online View Thread Recommend Forward

Flag as Inappropriate

Original Message:
Sent: 12-08-2022 15:59
From: Angela Killion
Subject: Employee training records/histories

Good afternoon!

The Arizona Department of Public Safety is looking for information on how other agencies track their employee's training records and histories.
If you wouldn't mind sharing how your agency tracks that information, we would appreciate your time.

Please send your responses directly to Sgt. Travis Meadows at tmeadows@azdps.gov and Trooper Carl Klaproth at cklaprothIII@azdps.gov.

Thank you!

Angela Killion
Administrative Services Officer
Arizona Department of Public Safety

You are subscribed to "State & Provincial Police Planning Officers Section SPPPOS" as liam.j.powers@state.ma.us. To change your subscriptions, go to My Subscriptions.
To unsubscribe from this community discussion, go to Unsubscribe.

From: IACP
To: Powers, Liam (POL)
Subject: State & Provincial Police Planning Officers Section SPPPOS Digest for Tuesday February 7, 2023
Date: Wednesday, February 8, 2023 12:29:36 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.

State & Provincial Police Planning Officers Section SPPPOS

Post New Message

Feb 7, 2023

Discussions

started 9 hours ago, Tom Walley (0 replies)

Fire Extinguishers Carried in Patrol Vehicles

1. The Missouri State Highway Patrol is requesting... Tom Walley

started 11 hours ago, Michael Hakey (0 replies)

Report Writing

Good morning/afternoon, We are looking at... Michael Hakey

started yesterday, Andrew Hyer (2 replies)

ALPR Policy/Guidance

3. Andrew, NSP does not utilize LPR/ALPR... Kevin Ryan
4. SDHP does not use that technology sir. ... Kevin Burke

started yesterday, Andrew Hyer (1 reply)

Case Management Software

Good Morning Lt. Hyer, SDHP uses... Kevin Burke

started yesterday, Michael Hakey (2 replies)

Pistol and Patrol Rifle Qualifications

6. Hello, SDHP qualifies on the regular duty... Kevin Burke

started 14 days ago, Joe Hall (7 replies)

Agency Pay Adjustment

Good morning, Joe. NSP has a collective... Kevin Ryan

started 2 months ago, Angela Killion (2 replies)

Employee training records/histories

8. Good morning, The Tennessee Highway... Sarah Hurst

top next

1. Fire Extinguishers Carried in Patrol Vehicles

Reply to Group Reply to Sender

Feb 7, 2023 2:32 PM
Tom Walley

The Missouri State Highway Patrol is requesting information on what type and size of fire extinguisher your patrol vehicles are equipped with. *Please respond directly to Sergeant Griggs at* Shawn.Griggs@mshp.dps.mo.gov

What type and sized are your patrol vehicles equipped with?

- "ABC" fire extinguisher ?
- Water fire extinguisher ?
- COLDFIRE fire extinguisher ?
- Other _____ ?
-
- What size fire extinguisher (Pounds/Gallons/Liters)

_____ ?

Lieutenant Tom Walley
Missouri State Highway Patrol
Research and Development Division

Reply to Group Online View Thread Recommend Forward
Flag as Inappropriate

top previous next

2. Report Writing

Reply to Group | Reply to Sender

Feb 7, 2023 12:29 PM
Michael Hakey

Good morning/afternoon,

We are looking at revising our Report Writing Manual and report writing lesson plans. Currently, we have both a Writing Manual and a Report Writing Manual. The Writing Manual is more for standardized guidelines for general writing for both professional staff and sworn personnel in terms of memos and letters, staff studies, etc. Basically the writing process. The Police Report Writing Manual is specific to sworn personnel for mechanics of report writing, writing offense reports, supplemental reports, etc. The report writing lesson plan is a part of the training troopers go through during the academy.

We are requesting from other agencies:

1) Any similar type of writing manuals.

2) Any report writing lesson plans and/or training materials.

Please send any responses either to myself at mhakey@azdps.gov or directly to this community message board.

Thank you.

Michael Hakey
Administrative Supervisor
Research & Planning Unit
Arizona Department of Public Safety
PO Box 6638, Mail Drop 1205
Phoenix, AZ 85005
(602) 223-2664

Reply to Group Online View Thread Recommend Forward

Flag as Inappropriate

3. Re: ALPR Policy/Guidance

Reply to Group | Reply to Sender

Feb 7, 2023 7:30 AM
Kevin Ryan

Andrew,

NSP does not utilize LPR/ALPR technology in our patrol cars.

Thank you,
Kevin

Kevin Ryan
Captain
Nebraska State Patrol
NE

Reply to Group Online | View Thread | Recommend | Forward

Flag as Inappropriate

Original Message:
Sent: 02-06-2023 18:35
From: Andrew Hyer
Subject: ALPR Policy/Guidance

The Wisconsin State Patrol is going to be activating the ALPR feature on our Fleet 3 cameras and is looking for information about the use of ALPR.

1. Does your agency use LPR/ALPR technology in squad cars?
2. What policies have been established for how the technology is used? Please share any policies or operating procedures.
3. How long is data from the system retained under your retention policy?

Thank you for the information in advance.

Andrew Hyer
Lieutenant
Special Operation Section
Wisconsin State Patrol
andrew.hyer@dot.wi.gov
(608) 316-0857
---

top previous next

4. Re: ALPR Policy/Guidance

Reply to Group | Reply to Sender

Feb 7, 2023 10:17 AM
Kevin Burke

SDHP does not use that technology sir.

Thanks, Kevin

Kevin Burke
Planning Officer
South Dakota Highway Patrol
kevin.burke@state.sd.us
605.641.1115

Reply to Group Online View Thread Recommend Forward

Flag as Inappropriate

Original Message:
Sent: 02-06-2023 18:35
From: Andrew Hyer
Subject: ALPR Policy/Guidance

The Wisconsin State Patrol is going to be activating the ALPR feature on our Fleet 3 cameras and is looking for information about the use of ALPR.

1. Does your agency use LPR/ALPR technology in squad cars?
2. What policies have been established for how the technology is used? Please share any policies or operating procedures.
3. How long is data from the system retained under your retention policy?

Thank you for the information in advance.

Andrew Hyer
Lieutenant
Special Operation Section
Wisconsin State Patrol
andrew.hyer@dot.wi.gov
(608) 316-0857
---

top previous next

5. Re: Case Management Software

Reply to Group | Reply to Sender

Feb 7, 2023 10:12 AM
Kevin Burke

Good Morning Lt. Hyer,

SDHP uses CentralSquare record management system.
Public Sector Safety & Administration Software

Thanks, Kevin

Kevin Burke
Planning Officer
South Dakota Highway Patrol
kevin.burke@state.sd.us
605.641.1115

Reply to Group Online View Thread Recommend Forward

Flag as Inappropriate

Original Message:
Sent: 02-06-2023 18:27
From: Andrew Hyer
Subject: Case Management Software

The Wisconsin State Patrol is exploring case management software for our investigative units. What case management software is your agency using?

Andrew Hyer
Lieutenant
Special Operation Section
Wisconsin State Patrol
andrew.hyer@dot.wi.gov
(608) 316-0857
---

top previous next

6. Re: Pistol and Patrol Rifle Qualifications

Reply to Group Reply to Sender

Feb 7, 2023 10:31 AM | view attached

Kevin Burke

Hello,

SDHP qualifies on the regular duty sidearm with the state mandated course. All sworn members are must shoot and pass that course. We have an additional course for backup guns. We did drop two additional SDHP sidearm qualification courses per year to allow for more training courses to be conducted.

There is not state mandated rifle course and SDHP shoots their own qualification course once a year.

Please see attached courses and please contact me for any questions. Email will be sent to Sgt. Mc Mains as well.

Thanks, Kevin

Kevin Burke
Planning Officer
South Dakota Highway Patrol
kevin.burke@state.sd.us
605.641.1115

Reply to Group Online **View Thread** **Recommend** **Forward**

Flag as Inappropriate

Original Message:
Sent: 02-06-2023 15:11
From: Michael Hakey
Subject: Pistol and Patrol Rifle Qualifications

Good afternoon,

Our Firearms Training Unit is requesting information about pistol and patrol rifle qualifications. We would like to know how many rounds are shot and what distance they are shot at for both pistol and patrol rifle qualifications. You can attach a qualification card (ours is attached) if it's easier.

We are asking for a tight turn-around of responses by February 17th. Please send your responses directly to Sgt. Dean McMains at dmcmains@azdps.gov.

You can also contact him directly at the same email or 602-223-2301 for any questions or if more information is required.

Thank you!

Michael Hakey

Administrative Supervisor
Research & Planning Unit
Arizona Department of Public Safety
PO Box 6638, Mail Drop 1205
Phoenix, AZ 85005
(602) 223-2664
---

top previous next

7. Re: Agency Pay Adjustment

Reply to Group Reply to Sender

Feb 7, 2023 7:52 AM
Kevin Ryan

Good morning, Joe.

NSP has a collective bargaining unit for troopers, investigators and sergeants. As part of the regular contract negotiations every two years, the bargaining unit was able to negotiate a 22% pay increase, in part to our agency being ranked 17th in the state for LE agencies.

We do not have retention bonuses, though the above ranks get a staggered longevity payment bases on years of service.

We do not offer sign-on or hiring bonuses or a referral program.

Thank you,
Kevin

Kevin Ryan
Captain
Nebraska State Patrol
NE

Reply to Group Online View Thread Recommend Forward
Flag as Inappropriate

Original Message:
Sent: 01-24-2023 15:45
From: Joe Hall
Subject: Agency Pay Adjustment

Good Afternoon Fellow Planners,

Louisiana State Police is in the process of preparing a request for a departmental pay adjustment, and is seeking information from other state agencies regarding the following information.

1. Have your agencies requested and/or received a pay adjustment within the past three years? What was the justification for the request?
2. Does your agency offer retention bonuses? If so, how are they structured?
3. Does your agency offer sign-on or hiring bonuses? How about an employee referral program where employees refer potential new hires, and the employee making the referral gets some "finder's fee" if employed?

As always we appreciate the communities assistance. Stay Safe!

Joe Hall
Sergeant
Louisiana Department of Public Safety
LA
---

top previous

8. Re: Employee training records/histories

Reply to Group | Reply to Sender



Feb 7, 2023 11:49 AM
Sarah Hurst

Good morning,

The Tennessee Highway Patrol utilizes a program called Training Traks to record all training. It's from IPTM out of Florida

---
Sarah Hurst
Sergeant
Tennessee Highway Patrol
TN

Reply to Group Online **View Thread** **Recommend** **Forward**

Flag as Inappropriate

Original Message:
Sent: 12-08-2022 15:59
From: Angela Killion
Subject: Employee training records/histories

Good afternoon!

The Arizona Department of Public Safety is looking for information on how other agencies track their employee's training records and histories.
If you wouldn't mind sharing how your agency tracks that information, we would appreciate your time.

Please send your responses directly to Sgt. Travis Meadows at tmeadows@azdps.gov and Trooper Carl Klaproth at cklaprothIII@azdps.gov.

Thank you!

Angela Killion
Administrative Services Officer
Arizona Department of Public Safety

You are subscribed to "State & Provincial Police Planning Officers Section SPPPOS" as liam.j.powers@state.ma.us. To change your subscriptions, go to My Subscriptions.
To unsubscribe from this community discussion, go to Unsubscribe.

From: IACP
To: O"Brien, Mark (POL)
Subject: State & Provincial Police Planning Officers Section SPPPOS Digest for Tuesday February 7, 2023
Date: Wednesday, February 8, 2023 12:28:33 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.

State & Provincial Police Planning Officers Section SPPPOS

Post New Message

Feb 7, 2023

Discussions

started 9 hours ago, Tom Walley (0 replies)

Fire Extinguishers Carried in Patrol Vehicles

1. The Missouri State Highway Patrol is requesting... Tom Walley

started 11 hours ago, Michael Hakey (0 replies)

Report Writing

Good morning/afternoon, We are looking at... Michael Hakey

started yesterday, Andrew Hyer (2 replies)

ALPR Policy/Guidance

3. Andrew, NSP does not utilize LPR/ALPR... Kevin Ryan
4. SDHP does not use that technology sir. ... Kevin Burke

started yesterday, Andrew Hyer (1 reply)

Case Management Software

Good Morning Lt. Hyer, SDHP uses... Kevin Burke

started yesterday, Michael Hakey (2 replies)

Pistol and Patrol Rifle Qualifications

6. Hello, SDHP qualifies on the regular duty... Kevin Burke

started 14 days ago, Joe Hall (7 replies)

Agency Pay Adjustment

Good morning, Joe. NSP has a collective... Kevin Ryan

started 2 months ago, Angela Killion (2 replies)

Employee training records/histories

8. Good morning, The Tennessee Highway... Sarah Hurst

top next

1. Fire Extinguishers Carried in Patrol Vehicles

Reply to Group | Reply to Sender

Feb 7, 2023 2:32 PM
Tom Walley

The Missouri State Highway Patrol is requesting information on what type and size of fire extinguisher your patrol vehicles are equipped with. *Please respond directly to Sergeant Griggs at* Shawn.Griggs@mshp.dps.mo.gov

What type and sized are your patrol vehicles equipped with?

- "ABC" fire extinguisher ?
- Water fire extinguisher ?
- COLDFIRE fire extinguisher ?
- Other _____ ?
-
- What size fire extinguisher (Pounds/Gallons/Liters)

_____ ?

Lieutenant Tom Walley
Missouri State Highway Patrol
Research and Development Division

Reply to Group Online View Thread Recommend Forward

Flag as Inappropriate

top previous next

2. Report Writing

Reply to Group | Reply to Sender

Feb 7, 2023 12:29 PM
Michael Hakey

Good morning/afternoon,

We are looking at revising our Report Writing Manual and report writing lesson plans. Currently, we have both a Writing Manual and a Report Writing Manual. The Writing Manual is more for standardized guidelines for general writing for both professional staff and sworn personnel in terms of memos and letters, staff studies, etc. Basically the writing process. The Police Report Writing Manual is specific to sworn personnel for mechanics of report writing, writing offense reports, supplemental reports, etc. The report writing lesson plan is a part of the training troopers go through during the academy.

We are requesting from other agencies:

1) Any similar type of writing manuals.

2) Any report writing lesson plans and/or training materials.

Please send any responses either to myself at mhakey@azdps.gov or directly to this community message board.

Thank you.

Michael Hakey
Administrative Supervisor
Research & Planning Unit
Arizona Department of Public Safety
PO Box 6638, Mail Drop 1205
Phoenix, AZ 85005
(602) 223-2664

Reply to Group Online View Thread Recommend Forward

Flag as Inappropriate

3. Re: ALPR Policy/Guidance

Reply to Group | Reply to Sender

Feb 7, 2023 7:30 AM
Kevin Ryan

Andrew,

NSP does not utilize LPR/ALPR technology in our patrol cars.

Thank you,
Kevin

Kevin Ryan
Captain
Nebraska State Patrol
NE

Reply to Group Online | View Thread | Recommend | Forward

Flag as Inappropriate

Original Message:
Sent: 02-06-2023 18:35
From: Andrew Hyer
Subject: ALPR Policy/Guidance

The Wisconsin State Patrol is going to be activating the ALPR feature on our Fleet 3 cameras and is looking for information about the use of ALPR.

1. Does your agency use LPR/ALPR technology in squad cars?
2. What policies have been established for how the technology is used? Please share any policies or operating procedures.
3. How long is data from the system retained under your retention policy?

Thank you for the information in advance.

Andrew Hyer
Lieutenant
Special Operation Section
Wisconsin State Patrol
andrew.hyer@dot.wi.gov
(608) 316-0857
---

top previous next

4. Re: ALPR Policy/Guidance

Reply to Group | Reply to Sender

Feb 7, 2023 10:17 AM
Kevin Burke

SDHP does not use that technology sir.

Thanks, Kevin

Kevin Burke
Planning Officer
South Dakota Highway Patrol
kevin.burke@state.sd.us
605.641.1115

Reply to Group Online View Thread Recommend Forward

Flag as Inappropriate

Original Message:
Sent: 02-06-2023 18:35
From: Andrew Hyer
Subject: ALPR Policy/Guidance

The Wisconsin State Patrol is going to be activating the ALPR feature on our Fleet 3 cameras and is looking for information about the use of ALPR.

1. Does your agency use LPR/ALPR technology in squad cars?
2. What policies have been established for how the technology is used? Please share any policies or operating procedures.
3. How long is data from the system retained under your retention policy?

Thank you for the information in advance.

Andrew Hyer
Lieutenant
Special Operation Section
Wisconsin State Patrol
andrew.hyer@dot.wi.gov
(608) 316-0857
---

top previous next

5. Re: Case Management Software

Reply to Group | Reply to Sender

Feb 7, 2023 10:12 AM
Kevin Burke

Good Morning Lt. Hyer,

SDHP uses CentralSquare record management system.
Public Sector Safety & Administration Software

Thanks, Kevin

Kevin Burke
Planning Officer
South Dakota Highway Patrol
kevin.burke@state.sd.us
605.641.1115

Reply to Group Online | View Thread | Recommend | Forward

Flag as Inappropriate

Original Message:
Sent: 02-06-2023 18:27
From: Andrew Hyer
Subject: Case Management Software

The Wisconsin State Patrol is exploring case management software for our investigative units. What case management software is your agency using?

Andrew Hyer
Lieutenant
Special Operation Section
Wisconsin State Patrol
andrew.hyer@dot.wi.gov
(608) 316-0857
---

top previous next

6. Re: Pistol and Patrol Rifle Qualifications

Reply to Group | Reply to Sender

Feb 7, 2023 10:31 AM | view attached

Kevin Burke

Hello,

SDHP qualifies on the regular duty sidearm with the state mandated course. All sworn members are must shoot and pass that course. We have an additional course for backup guns. We did drop two additional SDHP sidearm qualification courses per year to allow for more training courses to be conducted.

There is not state mandated rifle course and SDHP shoots their own qualification course once a year.

Please see attached courses and please contact me for any questions. Email will be sent to Sgt. Mc Mains as well.

Thanks, Kevin

Kevin Burke
Planning Officer
South Dakota Highway Patrol
kevin.burke@state.sd.us
605.641.1115

Reply to Group Online **View Thread** **Recommend** **Forward**

Flag as Inappropriate

Original Message:
Sent: 02-06-2023 15:11
From: Michael Hakey
Subject: Pistol and Patrol Rifle Qualifications

Good afternoon,

Our Firearms Training Unit is requesting information about pistol and patrol rifle qualifications. We would like to know how many rounds are shot and what distance they are shot at for both pistol and patrol rifle qualifications. You can attach a qualification card (ours is attached) if it's easier.

We are asking for a tight turn-around of responses by February 17th. Please send your responses directly to Sgt. Dean McMains at dmcmains@azdps.gov.

You can also contact him directly at the same email or 602-223-2301 for any questions or if more information is required.

Thank you!

Michael Hakey

Administrative Supervisor
Research & Planning Unit
Arizona Department of Public Safety
PO Box 6638, Mail Drop 1205
Phoenix, AZ 85005
(602) 223-2664
---

top previous next

7. Re: Agency Pay Adjustment

Reply to Group Reply to Sender

Feb 7, 2023 7:52 AM
Kevin Ryan

Good morning, Joe.

NSP has a collective bargaining unit for troopers, investigators and sergeants. As part of the regular contract negotiations every two years, the bargaining unit was able to negotiate a 22% pay increase, in part to our agency being ranked 17th in the state for LE agencies.

We do not have retention bonuses, though the above ranks get a staggered longevity payment bases on years of service.

We do not offer sign-on or hiring bonuses or a referral program.

Thank you,
Kevin

Kevin Ryan
Captain
Nebraska State Patrol
NE

Reply to Group Online View Thread Recommend Forward
Flag as Inappropriate

Original Message:
Sent: 01-24-2023 15:45
From: Joe Hall
Subject: Agency Pay Adjustment

Good Afternoon Fellow Planners,

Louisiana State Police is in the process of preparing a request for a departmental pay adjustment, and is seeking information from other state agencies regarding the following information.

1. Have your agencies requested and/or received a pay adjustment within the past three years? What was the justification for the request?
2. Does your agency offer retention bonuses? If so, how are they structured?
3. Does your agency offer sign-on or hiring bonuses? How about an employee referral program where employees refer potential new hires, and the employee making the referral gets some "finder's fee" if employed?

As always we appreciate the communities assistance. Stay Safe!

Joe Hall
Sergeant
Louisiana Department of Public Safety
LA
---

top previous

8. Re: Employee training records/histories

Reply to Group Reply to Sender



Feb 7, 2023 11:49 AM
Sarah Hurst

Good morning,

The Tennessee Highway Patrol utilizes a program called Training Traks to record all training. It's from IPTM out of Florida

---
Sarah Hurst
Sergeant
Tennessee Highway Patrol
TN

Reply to Group Online **View Thread** **Recommend** **Forward**

Flag as Inappropriate

Original Message:
Sent: 12-08-2022 15:59
From: Angela Killion
Subject: Employee training records/histories

Good afternoon!

The Arizona Department of Public Safety is looking for information on how other agencies track their employee's training records and histories.
If you wouldn't mind sharing how your agency tracks that information, we would appreciate your time.

Please send your responses directly to Sgt. Travis Meadows at tmeadows@azdps.gov and Trooper Carl Klaproth at cklaprothIII@azdps.gov.

Thank you!

Angela Killion
Administrative Services Officer
Arizona Department of Public Safety

You are subscribed to "State & Provincial Police Planning Officers Section SPPPOS" as mark.obrien@state.ma.us. To change your subscriptions, go to My Subscriptions.
To unsubscribe from this community discussion, go to Unsubscribe.

From: IACP
To: O"Brien, Mark (POL)
Subject: State & Provincial Police Planning Officers Section SPPPOS Digest for Wednesday February 22, 2023
Date: Thursday, February 23, 2023 12:18:27 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.

State & Provincial Police Planning Officers Section SPPPOS

Post New Message

Feb 22, 2023

Discussions

started 8 hours ago, Keitha Pritchard (0 replies)

EVOC and TIMs

1. Good afternoon, New Mexico State Police is... Keitha Pritchard

started 11 hours ago, Emily Perkins (4 replies)

Wrong-way pursuits

Good afternoon all: The Kentucky State... Emily Perkins
Good afternoon, The Vermont State Police... Timothy Gould
Wonderful, thank you so much! Emily M.... Emily Perkins
Hey Emily, Our policy states the below... Sarah Hurst
Afternoon, Our policy does not list wrong... Edward Larney

started 12 hours ago, Brina Gendhar (0 replies)

Civilians working in Crime Prevention

7. Good afternoon, The Michigan State... Brina Gendhar

started 16 days ago, Andrew Hyer (5 replies)

ALPR Policy/Guidance

Afternoon, we do not have carry them on patrol... Edward Larney
Lt Hyer, Please see the below responses... Sarah Hurst

started 2 months ago, Angela Killion (3 replies)

Employee training records/histories

10. At DSP, we print out their certificate or... Edward Larney

top next

1. EVOC and TIMs

Reply to Group Reply to Sender

Feb 22, 2023 3:55 PM
Keitha Pritchard

Good afternoon,

New Mexico State Police is requesting information from other agencies for EVOC and TIMs programs.

More specifically, does your agency have full-time or part-time EVOC and TIMs units/instructors? If you have a full-time unit how many are on it and how is it structured? If your agency has part-time instructors, how is your agency conducting the instruction (i.e. frequency of instruction to department personnel, requirements for instructors)?

Do you have any policies or directives for this?

Thank you,

KC Pritchard

New Mexico State Police

Keitha Pritchard
Officer
New Mexico State Police
NM

Reply to Group Online View Thread Recommend Forward

Flag as Inappropriate

2. Wrong-way pursuits

Reply to Group | Reply to Sender

Feb 22, 2023 12:58 PM
Emily Perkins

Good afternoon all:

The Kentucky State Police seem to be encountering more instances of becoming involved in pursuits traveling in the wrong direction on divided highways. We are hoping to obtain a copy of any policies, training materials, guidelines, legal decisions, or other information your agency may have specific to wrong-way driver pursuits. Please feel free to reply here or by email to emilym.perkins@ky.gov.

Thank you so much for your assistance with this topic.

Emily M. Perkins
Procedures Development Specialist
Strategic Planning Branch
Kentucky State Police
emilym.perkins@ky.gov

Reply to Group Online | View Thread | Recommend | Forward

Flag as Inappropriate

3. Re: Wrong-way pursuits

Reply to Group | Reply to Sender

Feb 22, 2023 1:07 PM | view attached

Timothy Gould

Good afternoon,

The Vermont State Police strictly prohibit our Troopers from pursuing in a wrong way direction. Our pursuit intervention tactics policy has separate standards than engaging in a pursuit, so Troopers can still deploy intervention tactics if the circumstances warrant.

I have attached a copy of each policy.

Thank you,

Lt. Tim Gould
Professional Standards
Vermont State Police

Reply to Group Online View Thread Recommend Forward
Flag as Inappropriate

Original Message:
Sent: 2/22/2023 12:58:00 PM
From: Emily Perkins
Subject: Wrong-way pursuits

Good afternoon all:

The Kentucky State Police seem to be encountering more instances of becoming involved in pursuits traveling in the wrong direction on divided highways. We are hoping to obtain a copy of any policies, training materials, guidelines, legal decisions, or other information your agency may have specific to wrong-way driver pursuits. Please feel free to reply here or by email to emilym.perkins@ky.gov.

Thank you so much for your assistance with this topic.

Emily M. Perkins
Procedures Development Specialist
Strategic Planning Branch
Kentucky State Police
emilym.perkins@ky.gov
---

4. Re: Wrong-way pursuits

Reply to Group | Reply to Sender

Feb 22, 2023 1:09 PM
Emily Perkins

Wonderful, thank you so much!

Emily M. Perkins
Strategic Planning Branch
Kentucky State Police

Reply to Group Online **View Thread** **Recommend** **Forward**

Flag as Inappropriate

Original Message:
Sent: 2/22/2023 12:58:00 PM
From: Emily Perkins
Subject: Wrong-way pursuits

Good afternoon all:

The Kentucky State Police seem to be encountering more instances of becoming involved in pursuits traveling in the wrong direction on divided highways. We are hoping to obtain a copy of any policies, training materials, guidelines, legal decisions, or other information your agency may have specific to wrong-way driver pursuits. Please feel free to reply here or by email to emilym.perkins@ky.gov.

Thank you so much for your assistance with this topic.

Emily M. Perkins
Procedures Development Specialist
Strategic Planning Branch

Kentucky State Police
emilym.perkins@ky.gov
---

top previous next

5. Re: Wrong-way pursuits

Reply to Group Reply to Sender

Feb 22, 2023 3:12 PM | view attached

Sarah Hurst

Hey Emily,

Our policy states the below language for wrong way pursuits. I have attached the entire policy as well. The below is on Page 9.

C. Patrol vehicles **shall only be used** for the purposes listed below **as a last resort and when deadly force is justified.**

The determination to use a patrol vehicle for the purposes listed below is the sole decision of the pursuing Member.

1. Pursuing a vehicle in a direction opposite to the flow of traffic on a divided highway, and
2. Ramming or forcing the suspect's vehicle off the roadway

Sarah Hurst | Sergeant
Research, Planning and Development
1150 Foster Avenue
Nashville, TN 37243
p. 615-854-6814
sarah.hurst@tn.gov
tn.gov/safety

Reply to Group Online View Thread Recommend Forward

Flag as Inappropriate

Original Message:
Sent: 2/22/2023 12:58:00 PM
From: Emily Perkins
Subject: Wrong-way pursuits

Good afternoon all:

The Kentucky State Police seem to be encountering more instances of becoming involved in pursuits traveling in the wrong direction on divided highways. We are hoping to obtain a copy of any policies, training materials, guidelines, legal decisions, or other information your agency may have specific to wrong-way driver pursuits. Please feel free to reply here or by email to emilym.perkins@ky.gov.

Thank you so much for your assistance with this topic.

Emily M. Perkins
Procedures Development Specialist
Strategic Planning Branch
Kentucky State Police
emilym.perkins@ky.gov
---

top previous next

6. Re: Wrong-way pursuits

Reply to Group Reply to Sender

Feb 22, 2023 3:28 PM | view attached

Edward Larney

Afternoon,

Our policy does not list wrong way pursuits as an automatic disqualifier technically,

however, based upon our guidelines, it would likely be terminated. I have attached our pursuit policy.

Edward Larney
Sergeant
Delaware State Police
DE

Reply to Group Online View Thread Recommend Forward
Flag as Inappropriate

Original Message:
Sent: 02-22-2023 12:57
From: Emily Perkins
Subject: Wrong-way pursuits

Good afternoon all:

The Kentucky State Police seem to be encountering more instances of becoming involved in pursuits traveling in the wrong direction on divided highways. We are hoping to obtain a copy of any policies, training materials, guidelines, legal decisions, or other information your agency may have specific to wrong-way driver pursuits. Please feel free to reply here or by email to emilym.perkins@ky.gov.

Thank you so much for your assistance with this topic.

Emily M. Perkins
Procedures Development Specialist
Strategic Planning Branch
Kentucky State Police
emilym.perkins@ky.gov

Reply to Group | Reply to Sender

Feb 22, 2023 11:47 AM
Brina Gendhar

Good afternoon,

The Michigan State Police is inquiring to see if any agencies use civilian members to complete crime prevention activities, for crime prevention purposes, and/or crime prevention related positions?

All responses may be directed to F/Lt. Brian McComb at MccombB1@michigan.gov

Thank you!

Brina

Brina Gendhar
Planning, Research, and Accreditation Section
Michigan State Police
Lansing, Michigan
517-719-4613
gendharb@michigan.gov

Reply to Group Online | View Thread | Recommend | Forward
Flag as Inappropriate

top previous next

8. Re: ALPR Policy/Guidance

Reply to Group | Reply to Sender

Feb 22, 2023 3:18 PM | view attached

Edward Larney

Afternoon, we do not have carry them on patrol vehicles, just at stationary locations. I have included our policy on these.

Edward Larney
Sergeant
Delaware State Police
DE

Reply to Group Online View Thread Recommend Forward
Flag as Inappropriate

Original Message:
Sent: 02-06-2023 18:35
From: Andrew Hyer
Subject: ALPR Policy/Guidance

The Wisconsin State Patrol is going to be activating the ALPR feature on our Fleet 3 cameras and is looking for information about the use of ALPR.

1. Does your agency use LPR/ALPR technology in squad cars?
2. What policies have been established for how the technology is used? Please share any policies or operating procedures.
3. How long is data from the system retained under your retention policy?

Thank you for the information in advance.

Andrew Hyer
Lieutenant
Special Operation Section
Wisconsin State Patrol
andrew.hyer@dot.wi.gov
(608) 316-0857
---

9. Re: ALPR Policy/Guidance

Reply to Group | Reply to Sender

Feb 22, 2023 3:29 PM | view attached

Sarah Hurst

Lt Hyer,

Please see the below responses from the Tennessee Highway Patrol.

1. Does your agency use LPR/ALPR technology in squad cars? Yes, some – We have 64 vehicles with LPR's
2. What policies have been established for how the technology is used? Please share any policies or operating procedures. Attached.
3. How long is data from the system retained under your retention policy? 90 Days

If you need any additional information please let me know.

Thanks,

Sarah Hurst | Sergeant
Research, Planning and Development
1150 Foster Avenue
Nashville, TN 37243
p. 615-854-6814
sarah.hurst@tn.gov
tn.gov/safety

Original Message:

Sent: 2/6/2023 6:35:00 PM
From: Andrew Hyer
Subject: ALPR Policy/Guidance

The Wisconsin State Patrol is going to be activating the ALPR feature on our Fleet 3 cameras and is looking for information about the use of ALPR.

1. Does your agency use LPR/ALPR technology in squad cars?
2. What policies have been established for how the technology is used? Please share any policies or operating procedures.
3. How long is data from the system retained under your retention policy?

Thank you for the information in advance.

Andrew Hyer
Lieutenant
Special Operation Section
Wisconsin State Patrol
andrew.hyer@dot.wi.gov
(608) 316-0857
---

top previous

10. Re: Employee training records/histories

Reply to Group | Reply to Sender

Feb 22, 2023 3:11 PM
Edward Larney

At DSP, we print out their certificate or training record and physically add it their personnel file.

Edward Larney
Sergeant
Delaware State Police
DE

Reply to Group Online View Thread Recommend Forward

Flag as Inappropriate

Original Message:
Sent: 12-08-2022 15:59
From: Angela Killion
Subject: Employee training records/histories

Good afternoon!

The Arizona Department of Public Safety is looking for information on how other agencies track their employee's training records and histories.
If you wouldn't mind sharing how your agency tracks that information, we would appreciate your time.

Please send your responses directly to Sgt. Travis Meadows at tmeadows@azdps.gov and Trooper Carl Klaproth at cklaprothIII@azdps.gov.

Thank you!

Angela Killion
Administrative Services Officer
Arizona Department of Public Safety

You are subscribed to "State & Provincial Police Planning Officers Section SPPPOS" as mark.obrien@state.ma.us. To change your subscriptions, go to My Subscriptions.
To unsubscribe from this community discussion, go to Unsubscribe.

From: CSAP DNG-ISAC
To: Keefe, Edward (POL)
Subject: TLPCLEAR: [PARTNER ADVISORY] Flashpoint: Daily Standup - October 27, 2023
Date: Friday, October 27, 2023 9:48:48 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.

PARTNER ADVISORY

Flashpoint: Daily Standup - October 27, 2023

TLP:CLEAR Oct 27, 2023

YoroTrooper: Researchers Warn of Kazakhstan's Stealthy Cyber Espionage Group (TheHackerNews)

Target audience: CISO, Incident Response, Security Ops, Threat Intel/CTI

- Summary: A relatively new threat actor known as YoroTrooper is likely made up of operators originating from Kazakhstan. The assessment, which comes from Cisco Talos, is based on their fluency in Kazakh and Russian, use of Tenge to pay for operating infrastructure, and very limited targeting of Kazakhstani entities, barring the government's Anti-Corruption Agency. "YoroTrooper

attempts to obfuscate the origin of their operations, employing various tactics to make its malicious activity appear to emanate from Azerbaijan, such as using VPN exit nodes local to that region," security researchers Asheer Malhotra and Vitor Ventura said. The adversary is known to be active since at least June 2022, singling out various state-owned entities in the Commonwealth of Independent States (CIS) countries. Slovak cybersecurity firm ESET is tracking the activity under the name SturgeonPhisher.

- Analyst comment: State-sponsored advanced persistent threat (APT) groups have traditionally been limited to countries such as Iran, China, and Russia. However, in recent years an increasing number of additional nations have also formed state-sponsored cyber threat groups to facilitate cyberespionage, sabotage, or intellectual property campaigns that align with national interests or geopolitical strategies.

See also:

- "Kazakhstan-Associated YoroTrooper Disguises Origin of Attacks as Azerbaijan" (Cisco Talos)
- "Kazakhstan Threat Landscape" (Flashpoint)

New iLeakage Attack Steals Emails, Passwords from Apple Safari (BleepingComputer)

Target audience: CISO, Security Ops, Threat Intel/CTI

- Summary: Academic researchers created a new speculative side-channel attack they named iLeakage that works on all recent Apple devices and can extract sensitive information from the Safari web browser. At core, it is a timerless Spectre attack that bypasses standard side-channel protections implemented by all browser vendors. iLeakage was developed by a team of academics from Georgia Tech, University of Michigan, and Ruhr University Bochum who examined Safari's side-channel resilience and managed to bypass existing countermeasures by implementing a timerless and architecture-agnostic method based on race conditions. By using speculative type confusion to bypass Apple's compressed 35-bit addressing and value poisoning countermeasures, the researchers could leak sensitive data from the target page, such as passwords and emails. The researchers used the same method to retrieve a

password for an Instagram test account that was auto-filled in the Safari web browser using the LastPass password management service. In another experiment, the researchers demonstrated how the iLeakage attacks also works on Chrome for iOS. They explain that Apple's policy forces all third-party iOS browsers to be overlays on top of Safari and use Apple browser's JavaScript engine.

- Analyst comment: According to Apple, the best preemptive mitigation strategy involves the following steps:

Enable Safari's hidden debug menu from Terminal.
Click on the debug menu in Safari.
Choose "WebKit Internal Features."
Check "Swap Processes on Cross-Site Window Open."

See also:

- iLeakage website
- "iOS and macOS Threat Landscape" (Flashpoint)

Nigerian Cybercrime Hub Shut Down with 6 Arrests (Dark Reading)

Target audience: Incident Response, Security Architects, Security Engineers, Security Ops, Threat Intel/CTI

- Summary: Nigerian police arrested six men they believe are associated with a cybercrime recruitment and mentoring hub. During interrogation, the six men - aged from 19 to 27 - admitted to activities including identity theft, hacking and trading of hacked Facebook accounts, romance scams, computer-related forgery, and other computer-related fraud, according to a statement from the Nigerian police force. Police also said intelligence reports indicated involvement by the syndicate in other high-level cybercrimes, including business email compromise and high-yield investment program fraud.
- Analyst comment: Internet scams and business email compromise operations have become increasingly sophisticated and organized as they are conducted by criminal syndicates that often operate similarly to regular companies, offering recruiting, training, and physical offices. The cybercrime and fraud syndicates often use their profits to bribe local law enforcement to ignore their illicit activities. However, it appears that the federal governments in Nigeria and some other countries have been cracking down on such operations.

See also:

- "PRESS RELEASE: NPF-NCCC SHUTDOWN CRIMINAL CYBERCRIME TRAINING AND OPERATIONAL CENTER, ARRESTS SIX THREAT ACTORS" (Nigeria Police Force, X)
- "Indian Federal Police Raid Tech Scam Centers" (FraudToday)
- "Nigeria Global Spotlight (Analyst Knowledge Page)" (Flashpoint)

Additional stories are included below, as they are of interest to threat intelligence teams:

- "Complex Spy Platform StripedFly Bites 1M Victims" (DarkReading)
- "Iranian Group Tortoiseshell Launches New Wave of IMAPLoader Malware Attacks" (TheHackerNews)
- "Hackers Attack Guatemalan Webpages in Support of Pro-Democracy Protests" (IndianCountryToday)
- "Record-Breaking 100 Million RPS DDoS Attack Exploits HTTP/2 Rapid Reset Flaw" (TheHackerNews)
- "Microsoft Warns as Scattered Spider Expands from SIM Swaps to Ransomware" (TheHackerNews)
- "France Says Russian State Hackers Breached Numerous Critical Networks" (BleepingComputer)
- "Chilean Telecom Giant GTD Hit by the Rorschach Ransomware Gang" (BleepingComputer)
- "Seiko Says Ransomware Attack Exposed Sensitive Customer Data" (BleepingComputer)
- "'Sam Bankman-Fried's Jurors Were Sent Home for the Day, but His Debut on the Stand Was Significant Anyway" (CoinDesk)
- "Media Reported Hamas Got Millions via Crypto, but the Data Provider They Cited Says It Was Misconstrued" (CoinDesk)
- "50% of US Homes Have a Security System" (SecurityMagazine)
- "New Orleans Deploys ALPR Tech to Help Secure the French Quarter" (SecurityMagazine)
- "3 Ways Mexican Organized Crime Affects Foreign Investment" (InsightCrime)
- "Online Gaming Safety Alert: 11-Year-Old Girl Kidnapped after Contact on Roblox" (SafeWise)
- "Philadelphia Cyberattack Compromised Health Data of City Employees" (CyberScoop)
- "Police Seize Ragnar Locker Leak Site" (CyberScoop)
- "DC Board of Elections Breach May Include Entire Voter

Roll" (CyberScoop)
- "US Senator Quizzes 23andMe over Credential-Stuffing Hack" (HealthcareInfosecurity)
- "SG-Based Protos Labs Nets $2.2m to Take Cybercrime Insurance to Vietnam" (TechInAsia)

Please find past standups at https://fp.tools/home/intelligence/standup.
Sign up for a free trial: https://go.flashpoint-intel.com/access/Cyware

View Alert

Download DNGISAC's Information Sharing App from.

If you are not supposed to receive this email, please contact us at **jbryk@dngisac.com,jcmartin@dngisac.com,mrecinos@dngisac.com**

To unsubscribe from future alerts, click here

Powered by Cyware

From: P1 Product Alert
To: McCarthy, Steven (POL)
Subject: Using smart tech for speed enforcement and improve community safety
Date: Tuesday, August 15, 2023 12:17:12 PM

August 15, 2023 | View as webpage | Too many emails? Update Subscription Preferences

Using smart technologies to curb reckless drivers, slow speeders and improve community safety

Speed cameras and ALPR make the job more efficient

Sponsored by Jenoptik

FEATURED CONTENT

Why America is falling behind on traffic safety

Compared to other nations, the U.S. is a far more dangerous place for pedestrians, cyclists and motorists.





A different 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.

Slower drivers mean faster progress toward vision of zero traffic deaths

LPR plus traffic data management systems can reduce the traffic enforcement workload for understaffed police departments.





How license plate recognition (LPR) can be a force multiplier

LPR plus traffic data management systems can reduce the traffic enforcement workload for understaffed police departments.

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 © 2023 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Video: Chief deputy went 96 in 35 mph zone; Metro Nashville PD"s SRO staffing
Date: Friday, July 14, 2023 4:31:51 PM

July 14, 2023 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Are you interested in learning new strategies and tactics to overcome wellness-related challenges?

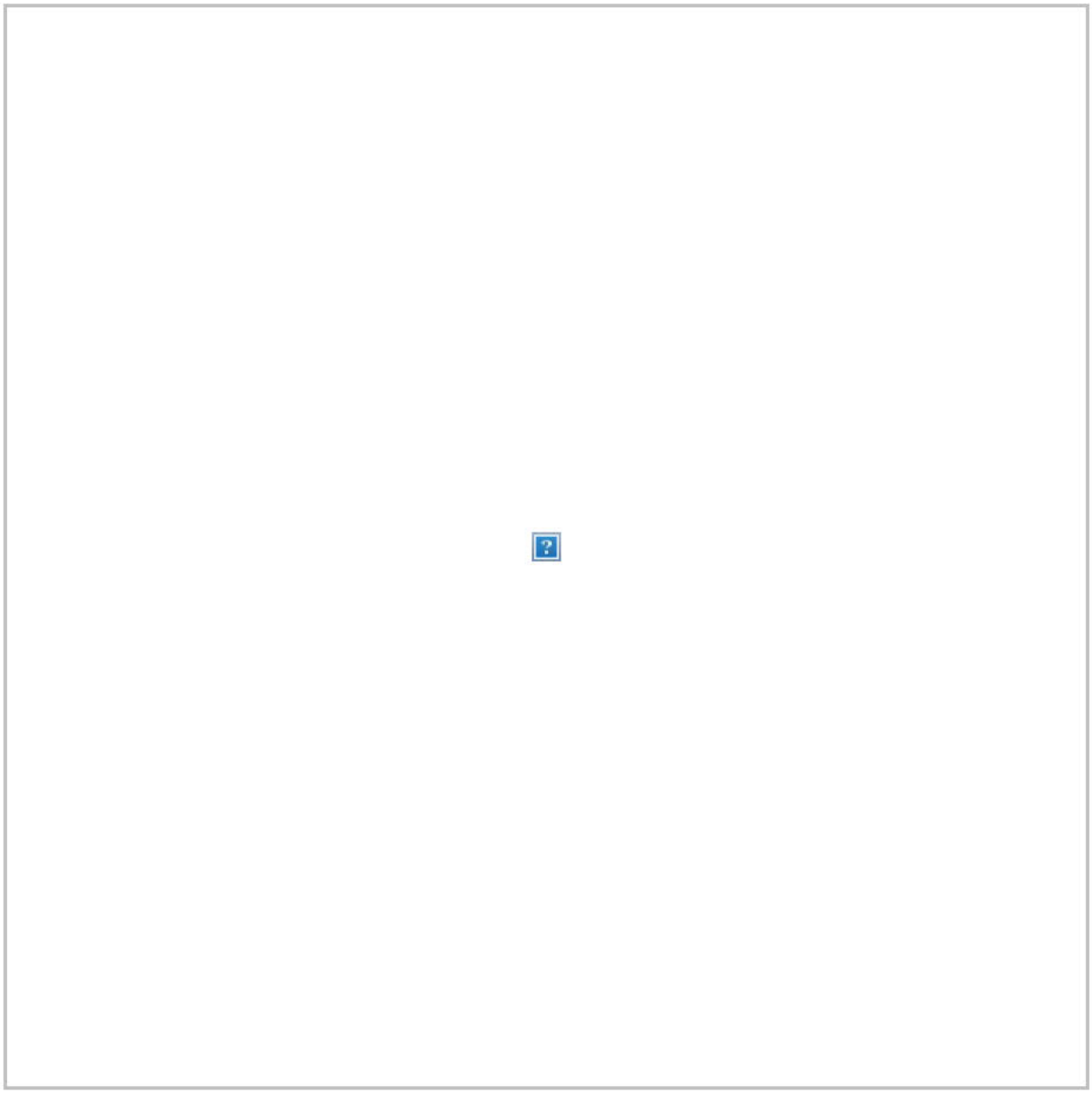
Register for a free webinar on July 18 at 11 a.m. CT to learn how to leverage foundational, world-class leadership principles developed by U.S. retired Navy SEAL Jocko Willink and former U.S. Navy SEAL Leif Babin. These two experts will discuss the inherent challenges that first responders face, including high-pressure shift work, ever-changing job demands and daily exhaustion.

Moreover, participants can expect to learn about how a healthy lifestyle can produce physiological and psychological benefits that increase first responder readiness and resilience.

Reserve your seat here.

Stay safe,

— *The Police1 Team*



Video: Chief deputy pulled over in unmarked department-issued vehicle

The chief deputy, who was in the car with another sheriff's office employee in

uniform, was cited for going 96 in a 35 mph zone

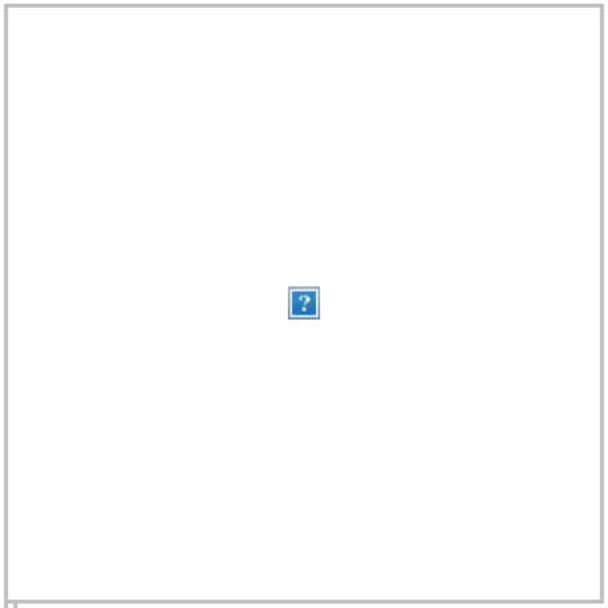
Ind. inmate charged with murder in deputy's strangulation death, faces death penalty

Metro Nashville PD 'not staffed to provide full-time SROs at elementary schools'

Judge approves Minneapolis police reform deal

LVMPD officer's brother testifies against him, says they rehearsed for $73K casino heist

Detroit police commish resigns amid prostitution scandal



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

#FITNESSFRIDAY

Ice bath therapy for law enforcement: Physical and mental benefits of cold water

By Joshua Lee, MA, MALST, CFE, CAMS, CCCI, CTFI, CCIE

Are you ready to take the plunge? Learn how ice bath therapy can benefit

police officers in their everyday lives as well as on duty

Musculoskeletal injuries: The most common type of injuries sustained in law enforcement

By Daniel Borowick

Lower body injuries, such as knee pain and lower back pain, are found present to a high degree in the law enforcement community

The impact of Barry Bonds, baseball player, on digital forensics

Join us to learn the surprising ways Barry Bonds influenced the world of digital forensics.

Register for the webinar - Thursday, August 3 (2 p.m. ET)

Lexipol Annual Conference: Closing Keynote by Gordon Graham!

Chose from 10 sessions designed for professionals in law enforcement. Topics include recruitment, legislative trends, policy, tactics, training, wellness, accreditation and more!

Register Free Now

PHOTO OF THE WEEK

We all scream for 'Operation Copsicle'

"Operation Copsicle" was created to celebrate the outgoing class of fifth-graders transitioning into middle school with a sweet treat

POLICE1 COLUMNIST SPOTLIGHT: LT. DAN MARCOU

Developing a respect-based police survival



attitude

By Lt. Dan Marcou

Respect may be the most important thing that contributes to an officer's safety – here's why



Deputy Eddy Luna's fight for physical and emotional survival after the gun smoke cleared

By Lt. Dan Marcou

"Everything was in slow motion, and I saw a flash. Suddenly I was down on my stomach, but I didn't even know I was shot."



How to avoid 'abject failure' in your in-progress mass murder response

By Lt. Dan Marcou

Initial responding officers must evaluate quickly, move to the sound of the guns, gathering intelligence on the move

Sponsored Content

The Alternative hits the streets in Texas

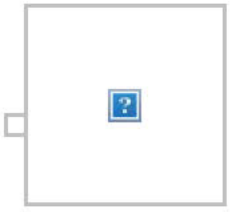
The Jackson County Sheriff's Office has become the first agency to adopt Alternative Ballistics' novel new less-lethal option.



FEATURED JOB

Juvenile Detention Officer Entry Level & Lateral

Up to $25,000 hiring incentive. Competitive pay and benefits. $31.16 - $39.46 Hourly





FEATURED EDUCATION

Enroll now at CCU; an online university!

CCU offers a 10% Tuition Discount; click the link for details. Plus, CCU offers interest-free payment plans! DEAC Accredited



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 © 2023 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Video: Dallas PD robot ends standoff; More NYPD cruisers going electric
Date: Thursday, January 5, 2023 1:29:17 PM

January 5, 2023 | View as webpage | Too many emails? Update Subscription Preferences

TOP STORIES

Nearly 1K NYC government vehicles becoming all-electric — including NYPD patrol cars

Mayor Eric Adams said his administration has already surpassed its 2025 goal for electrifying the fleet

Ind. police stopped Idaho slayings suspect twice on road trip so FBI could see his hands

N.J. officer indicted on misconduct charges in man's death during 2020 arrest

Video: Dallas PD robot helps end 6-hour standoff with suspect at golf course

Denver officer indicted on assault charges in shooting that injured 6 bystanders

'I had to come back': Calif. sergeant returns to work after leg amputation

Introducing the NEW Beretta APX A1

The Beretta APX A1 brings an improved trigger and every performance-enhanced feature to bear in the fastest, most comfortable striker-

fired pistol ever made.

Learn more

FEATURED CONTENT



Dr. Paul Taylor on what the research says about officer decision-making under stress

By Policing Matters

Understanding the causal factors behind officer performance is critical to informing police training



Today's police leadership paradigm: Toddlers leading babies

By Hank Prim

Amid the police recruitment and retention crisis, agencies need new techniques to transform officers into leaders

5 common myths about the online privacy of LEOs



Here's how cops can protect themselves, their families and take back their privacy.

Protect yourself now

TRAFFIC STOP SAFETY

One of the most important officer safety tactics I learned in the police academy

By Gordon Graham

Fifty years ago I was taught that the right-side approach on a traffic stop is the safest – and that message is just as relevant for recruits today

2 traffic stops, 2 very different outcomes

By Charles Remsberg

What made the life-and-death difference between two traffic stops on the same offender?

SPONSORED CONTENT

New ALPR system puts dent in Ohio city's crime

In Bowling Green an advanced new system provides not just still images but reviewable video and advanced analysis of passing vehicles – and that's helping solve a lot of cases.

FEATURED JOB

MPD Entry-Level & Lateral Officer Positions Available
Apply Today!

FEATURED RESOURCES

How to Buy Investigation Software (eBook)
Download 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: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Watch: One-handed shooting skills; Perfect score at LAPD"s bonus course
Date: Monday, June 19, 2023 5:02:26 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.

June 19, 2023 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

In this special edition of the Police1 member newsletter, we focus on the importance of maintaining and honing your firearms skills.

As you know, proficiency with firearms is not just about hitting a target; it's a vital part of ensuring safety – for yourself, your fellow officers and the community you serve. This ability does not come without regular, mindful practice. The unpredictable nature of law enforcement calls for quick thinking and action. Regular firearms training enhances your ability to neutralize threats effectively and safely.

In addition, we review some of the latest firearms to hit the market and provide some buying resources for firearms training, optics and more.

Stay safe,

— *The Police1 Team*

FIREARMS TRAINING

Lessons learned while building the ultimate RDS train-the-trainer class

By Ron LaPedis

Rangemaster Sgt. David Weidner and his staff run bi-monthly, two-day train-the-trainer classes for other agencies

Video: Firearms training drill breaks down high-stakes hostage situation

By Todd Fletcher

"The officer that took that shot, under that kind of stress, that guy saved lives. That's a guy I'd like to shake his hand."

When it comes to firearms training, it's all about the skills, not the drills

By Leon Reha

If you're practicing the stages of a test repeatedly you are not effectively training for anything at all

Why focused training on one-handed shooting drills is crucial to officer survival

By Todd Fletcher

Don't make a bad day worse by failing to practice the shooting skills that could help you prevail

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

FIREARMS REVIEWS

Field testing Springfield Armory's DS1911 Prodigy pistols

By Andrew L. Butts

These pistols use the traditional slide and barrel configuration of the tried-and-true 1911 and combine them with a double-column magazine

Why Smith & Wesson's Equalizer is not only for 1911



enthusiasts

By Kevin McPherson

I'm thoroughly impressed with how this gun handles, the features it has and the value it offers



Beretta APX A1: Reporting for duty

By Todd Fletcher

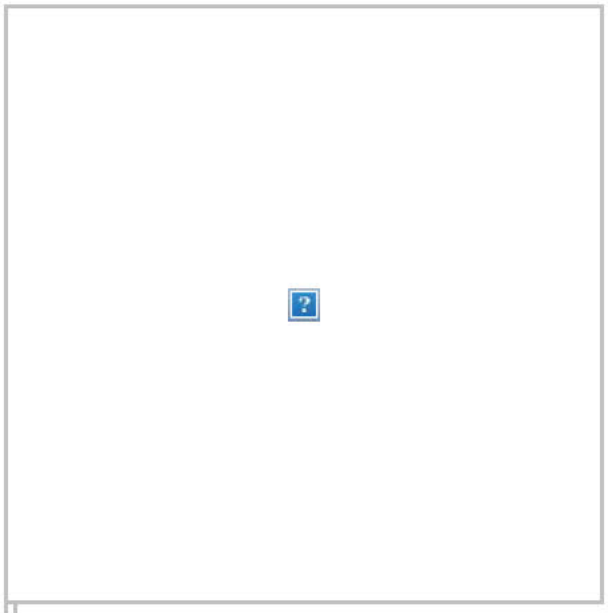
I would trust my life to this handgun, and I can think of no higher endorsement



How this LAPD officer achieved a perfect score

By Laura Neitzel

Motivation, practice and an accurate weapon are key



How one agency eased the burden of vehicle crash reporting



Longmont PD adopted these tech tools to create new efficiencies and clear crashes faster

Read more

HOW TO BUY GUIDES

How to buy firearm optics



By Police1 Staff
For the uninitiated, the variety of available firearms optics can be confusing; this guide can help



How to buy firearms

By Police1 Staff
Download this buying guide to learn key steps for product selection, purchasing and implementation



How to buy firearms training equipment

By Police1 Staff
Whether you're leading a purchase for the first time or looking to upgrade your PD's equipment, this is a starting point for your purchasing process



How to buy firearms storage

By Police1 Staff
Secure weapons storage has never been as important as it is today; here's what to consider in the acquisition of storage solutions to secure firearms



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 © 2023 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

To: Aumais, Matthew (POL)
Cc: Comeau, Melissa (POL); Rust, Rebecca (POL); Peterson, Stephanie G. (POL)
Subject: 2020 Heroin GAM - Need To-From
Date: Wednesday, August 23, 2023 12:57:54 PM
Attachments: Wish List Purchases for 2020 COPS Heroin.pdf
2020 COPS AHTF GAM Aug 2023 with edits KH-JL-MC.docx

Hi Matt,

We have incorporated the wish list items (see attached) in the new GAM. Right now we are waiting for the To-From for Oculus kits, NOMOS WIFI and additional hard drives.

Please let me know if I should reach out to Lt. George for a To-From or you will follow up with him directly?

Thank you,

Jeff Ly
Accountant IV – Grants
Massachusetts State Police
470 Worcester Road
Framingham, MA 01712
508-988-7081
Jeff.Ly@pol.state.ma.us

From: Ly, Jeff (POL)
To: Aumais, Matthew (POL)
Cc: Comeau, Melissa (POL); Rust, Rebecca (POL); Peterson, Stephanie G. (POL)
Subject: 2020 Heroin GAM - Need To-From
Date: Wednesday, August 23, 2023 12:58:43 PM
Attachments: Wish List Purchases for 2020 COPS Heroin.pdf
2020 COPS AHTF GAM Aug 2023 with edits KH-JL-MC.docx

Hi Matt,

We have incorporated the wish list items (see attached) in the new GAM. Right now we are waiting for the To-From for Oculus kits, NOMOS WIFI and additional hard drives.

Please let me know if I should reach out to Lt. George for a To-From or you want to follow up with him directly?

Thank you,

Jeff Ly
Accountant IV – Grants
Massachusetts State Police
470 Worcester Road
Framingham, MA 01712
508-988-7081
Jeff.Ly@pol.state.ma.us

To: Reeves, Talmadge (BER)
Subject: 2020 MSP Policies
Date: Friday, July 14, 2023 5:20:07 PM
Attachments: POLICIES PROCEDURES UPDATED 2020.pdf
image001.png

Talmadge – sorry for delay. See attached. Sean

Sean W. Farrell
Counsel III - Office of the Chief Legal Counsel
Massachusetts Department of State Police
470 Worcester Road
Framingham, MA 01702
(508)820-2153

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: Rust, Rebecca (POL)
To: LASHAWN.BENTON2@USDOJ.GOV
Cc: Comeau, Melissa (POL); Ly, Jeff (POL)
Subject: 2020HPWX0004 GAM
Date: Wednesday, October 18, 2023 1:13:00 PM
Attachments: 2020 COPS AHTF GAM Oct 2023 FINAL.docx

Good afternoon:
We just submitted a GAM in just grants for 2020HPWX0004, Anti-Heroin Task Force 2020. I have attached the letter that was attached. My apologies, our prior grant manager was Judith Williford, and the documentation in Just Grants is addressed to her. Let us know if there is anything else you need to get this moving. We are available to answer any questions you my have.

Thanks so much!

Rebecca Rust
Deputy Director of Grants and Special Projects
Massachusetts State Police
470 Worcester Road
Framingham, MA 01712
508-820-2688
Rebecca.Rust@pol.state.ma.us

Your feedback is important to us. We value your input to continuously improve and provide you with the best possible service.
Please let us know how we are doing by taking our short survey at the following link:
MSP Crime Laboratory Service Satisfaction Survey

All communications sent or received by this Commonwealth of Massachusetts email address may be subject to disclosure under the Massachusetts Public Records Law (M.G.L. Chapter 66, Section 10) and the Federal Freedom of Information Act.
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: Gouveia, Kim (NOR)
To: "arotella@acton-ma.gov"; "skrug@actonma.gov"; "chodges@actonma.gov"; "cbrowne@actonma.gov"; "Lgower@actonma.gov"; "nmeuse@actonma.gov"; Moriarty, Dan; "bharutunian@CambridgePolice.Org"; "cponte@cambridgepolice.org"; Blodgett, Jeff; Carlo, Wiliam; "jyoung@concordma.gov"; Harrington, Keith; "Cpaladino@concordma.gov"; "Drodriguez@concordma.gov"; Frink, Ryan P. (DOC); Beach, Fletcher D. (DOC); Borges, Matthew (DOC); Millar, Jonathan (DOC); Tully, Matt; "kmg@framinghamma.gov"; "kpursell@framinghamma.gov"; "smf@framinghamma.gov"; "Robert Kotowski"; DiGiorgio, Bryan; Chaisson, Jeffrey; "cducharme@lexingtonma.gov"; "AGolner@lowellma.gov"; "DPerrinJr@lowellma.gov"; "MTrani@lowellma.gov"; "MCassella@lowellma.gov"; "JSann@lowellma.gov"; "ledmonds@marlborough-ma.gov"; Odom Eang; "tracy.hornsby@massgaming.gov"; "geu_patrick.dimartino@massgaming.gov"; "ronald.alonso@massgaming.gov"; Hayes, Eric (POL); Loftus, Christopher (POL); Orlando, Giovanni (POL); "melnik@natickpolice.com"; "lanoue@natickpolice.com"; Halloran, Michelle; "arichard@sherbornpolice.org"; "jcosta@police.somerville.ma.us"; "rpasqualino@police.somerville.ma.us"; "glegros@police.somerville.ma.us"; Monaco, Alan; "bfitzpatrick@stow-ma.gov"; "mmoriarty@police.waltham.ma.us"; "jmcmeekin@police.waltham.ma.us"; "cvbastarache@police.waltham.ma.us"; "bsmith@wayland.ma.us"; Hebert, Mark; "nnicoletti@westfordma.gov"
Cc: Johnsen, Melissa (NOR); Gouveia, Kim (NOR)
Subject: 2022-23 Police Training Manual & Agenda
Date: Monday, February 6, 2023 4:45:11 PM
Attachments: SW Training Agenda 2.8.23 - PDF.pdf
2022-2023 Police Training Manual.pdf

Hello,

Attached please find the 2022-2023 Police Training Manual and the Agenda for our Police Training Program being held, Wednesday, February 8th. Thank you!

Kim Gouveia
Administrative Assistant to
Thomas D. Ralph, Chief Appeals & Training Bureau
Middlesex County District Attorney's Office
15 Commonwealth Avenue
Woburn, MA 01801
Phone: 781-897-6870
Fax: 781-897-6826

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:	Gouveia, Kim (NOR)
To:	Gallagher, Bryan; Flaherty, David; "Kevin Doherty"; "Brittany Zaccagnini"; "abongiorno@cambridgepolice.org"; "mgdonovan@cambridgepolice.org"; "tPasquarello@cambridgepolice.org"; "jlaracuente@cambridgepolice.org"; Brown, Dave; "KBAXTER@carlislepolice.com"; "Jroark@chelmsfordma.gov"; Cormier, Laurie (DOC); "cmcginty@framinghamma.gov"; "cnormandin@hopkintonpd.org"; Chang, Jose; avey; "barrett@hollistonpolice.com"; "aschofield@hopkintonpd.org"; "mlatour@hopkintonpd.org"; "cnormandin@hopkintonpd.org"; "nsaletnik@hopkintonpd.org"; "astewart@hopkintonpd.org"; Sowle, Mike; Evelyn, Aiden; "khankins@lexingtonma.gov"; cdunbar@lexingtonma.gov; "asepe@lowellma.gov"; "TFenlon@lowellma.gov"; "JBorodawka@lowellma.gov"; "RRichard@lowellma.gov"; "MQuinones@lowellma.gov"; "JPhothimath@lowellma.gov"; "kdeschenes1016@gmail.com"; "Kakouch@Lynnpolice.org"; "sdeciero@marlborough-ma.gov"; "mney@marlborough-ma.gov"; "mgiaquinto@marlborough-ma.gov"; "prichardson@marlborough-ma.gov"; "alarose@marlborough-ma.gov"; "bcox@marlborough-ma.gov"; "jbonina@marlborough-ma.gov"; Taylor, Dewayne (EEA); O"Keefe, Patrick R (POL); Gordon, Jeffrey (POL); "amccann@maynardpolice.com"; "RCubelli@ci.methuen.ma.us"; "Tnoonan@ci.Methuen.Ma.us"; "LMay@ci.methuen.ma.us"; "dvacca@newtonma.gov"; "erosenba@newtonma.gov"; "lkeefe@newtonma.gov"; "jpanica@newtonma.gov"; "jlau@newtonma.gov"; Jeffrey Boudreau; "jmclaughlin@newtonma.gov"; "zraymond@newtonma.gov"; "mcolella@newtonma.gov"; "ahenrickson@newtonma.gov"; "rabate@ci.reading.ma.us"; "mfaria@police.somerville.ma.us"; Catatao, Ashley; "fcicerone@police.somerville.ma.us"; "sdottin@police.somerville.ma.us"; Sheehan, Sean; "kleguisamon@police.somerville.ma.us"; "rkennedy@stoneham-ma.gov"; "dryan@stoneham-ma.gov"; "LdeZago@Stow-Ma.Gov"; "ckusz@stow-ma.gov"; "jgiles@townsendpd.org"; "clow@townsendpd.org"; Richard DiNanno; Kenneth Silva; Bartolomucci, John; "mmartino@police.watertown-ma.gov"; "kswift@police.watertown-ma.gov"; "connarton.k@police.westonma.gov"; "carlo.w@police.westonma.gov"; "connarton.k@police.westonma.gov"
Cc:	Johnsen, Melissa (NOR); Gouveia, Kim (NOR)
Subject:	2022-23 Police Training Manual, Agenda & Zoom Link
Date:	Monday, February 6, 2023 4:45:38 PM
Attachments:	2022-2023 Police Training Manual.pdf SW Training Agenda 2.8.23 - PDF.pdf

---

Hello,

Attached please find the 2022-2023 Police Training Manual, Agenda and link for the ZOOM below, for our Police Training Program being held, Wednesday, February 8th. Thank you!

Topic: Police Training
Time: Feb 8, 2023 08:30 AM Eastern Time (US and Canada)

Join Zoom Meeting
https://us02web.zoom.us/j/82509457258?pwd=aWJ4ditDSHNKZ2pBck9GQmY3b2Q5QT09

Meeting ID: 825 0945 7258
Passcode: 959903

Kim Gouveia
Administrative Assistant to
Thomas D. Ralph, Chief Appeals & Training Bureau
Middlesex County District Attorney's Office
15 Commonwealth Avenue
Woburn, MA 01801
Phone: 781-897-6870
Fax: 781-897-6826

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: Nason, Nicholas (POL)
To: Pack, Noah (POL); Banik, John (POL)
Cc: Warren, Rosemary (POL)
Subject: 2023 Annual Report
Date: Friday, February 17, 2023 3:25:00 PM
Attachments: 2023 ACISS Annual Report ACISS and LPR.docx

Lt. Banik and Sgt. Pack

Attached is the 2022 Annual Report, I made changes for the ACISS paragraphs. Please review the ACISS ones and make your changes for LPR (unless you already did your own).

Sergeant Nicholas Nason #2900
Massachusetts State Police
Division of Homeland Security & Preparedness
nicholas.nason@mass.gov
Phone: (508) 988-7305
Cell: [redacted]

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 message in error, please delete this email immediately.

To: Condlin, Christopher (POL); Powers, Liam (POL)
Subject: ALPR Accreditation Requirements
Date: Wednesday, May 31, 2023 11:33:54 AM
Attachments: ALPR MPAC Requirements.docx
image001.png

Chris,

Attached is the Accreditation standard related to ALPR technology. I read the policy and all of the pertinent points are addressed within the policy. There is a small formatting issue under the hit/alert confirmation section, the sub-bullet should be an open circle bullet point, not the dash. Could you please add the standard # into the reference section as follows: MPAC: 41.3.9.

Any questions let me know.

BP

Bill Pinkes
Accreditation Manager
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-808-3448

From: Pinkes, William (POL)
To: Condlin, Christopher (POL); Powers, Liam (POL)
Subject: ALPR Accreditation Requirements
Date: Wednesday, May 31, 2023 11:34:02 AM
Attachments: ALPR MPAC Requirements.docx
image001.png

Chris,

Attached is the Accreditation standard related to ALPR technology. I read the policy and all of the pertinent points are addressed within the policy. There is a small formatting issue under the hit/alert confirmation section, the sub-bullet should be an open circle bullet point, not the dash. Could you please add the standard # into the reference section as follows: MPAC: 41.3.9.

Any questions let me know.

BP

Bill Pinkes
Accreditation Manager
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-808-3448

To: Pack, Noah (POL)
Cc: Gray, Kellie (POL); Aumais, Matthew (POL); Ly, Jeff (POL); Silva, Kyra (POL)
Subject: ALPR bid from Motorola - COPS Heroin Grant
Date: Thursday, March 23, 2023 11:46:42 AM
Attachments: datasheet-axis-q1700-le-license-plate-camera-en-US-388197.pdf
Industrial LTE Router Airlink RV55 Sierra Wireless.pdf
Motorola Solutions Quote BD-23-1084-POLGH-GHQ-85837.pdf
VSS22-CovertEnclosures-072822-DIGITAL.pdf

Hi Sgt Pack.

We had one bid response to our request for quotes under PSE01 for ALPRs. Please see attached bid documents from Motorola. This purchase is funded with the FFY2020 COPS Heroin grant and the budget has $161,000 allocated.
The total of this quote is $171,549. You may need to reduce the number of cameras to be ordered or reach out to Motorola to see if they can sharpen their pencil. Please also confirm that the quote meets our requirements and includes everything needed. If there will be out-year costs, you should submit a To/From through your chain of command to request funds. Once you get the final quote, please have it approved/signed and return to me to issue a purchase order.
Let me know if I can be of any assistance.
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: Pack, Noah (POL)
Cc: Gray, Kellie (POL); Aumais, Matthew (POL); Ly, Jeff (POL); Silva, Kyra (POL)
Subject: ALPR bid from Motorola - COPS Heroin Grant
Date: Thursday, March 23, 2023 11:49:39 AM
Attachments: datasheet-axis-q1700-le-license-plate-camera-en-US-388197.pdf
Industrial LTE Router Airlink RV55 Sierra Wireless.pdf
Motorola Solutions Quote BD-23-1084-POLGH-GHQ-85837.pdf
VSS22-CovertEnclosures-072822-DIGITAL.pdf

Hi Sgt Pack.

We had one bid response to our request for quotes under PSE01 for ALPRs. Please see attached bid documents from Motorola. This purchase is funded with the FFY2020 COPS Heroin grant and the budget has $161,000 allocated.
The total of this quote is $171,549. You may need to reduce the number of cameras to be ordered or reach out to Motorola to see if they can sharpen their pencil. Please also confirm that the quote meets our requirements and includes everything needed. If there will be out-year costs, you should submit a To/From through your chain of command to request funds. Once you get the final quote, please have it approved/signed and return to me to issue a purchase order.
Let me know if I can be of any assistance.
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: Staples, Jennifer (POL)
To: Kwon, Gina K. (EPS); Terrey, Susan (EPS); Walker, Suleyken (EPS); Melander, John (EPS)
Subject: ALPR Cameras and FLOCK
Date: Wednesday, September 6, 2023 12:45:50 PM
Attachments: image001.png

Hi All:

Could we schedule a time next week to discuss with Colonel Cyr and the ALPR folks MSP purchasing a FLOCK ALPR Camera subscription? Not FLOCK cameras, but a subscription in order to access data.

Sue, I included you because you were originally involved in ALPR cameras, but feel free to bow out. ☺

Let me know if maybe Tuesday or Wednesday work.

Thanks!!

Jennifer M. Staples
Chief Legal Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Tel: (508) 820-2307
Cell: [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: Serra, Anthony F (POL)
To: Warren, Rosemary (POL)
Subject: ALPR Policy -
Date: Monday, October 2, 2023 3:05:23 PM
Attachments: TRF-11 Automatic License Plate Recognition (5).pdf
TRF-11 Automatic License Plate Recognition (6).pdf

Hi Rose,

Do you have a copy of the ALPR policy in effect in April of 2020? I was only able to locate the 2 attached policies. Thank you very much.

Anthony Serra
Staff Legal Counsel
Office of Chief Legal Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Telephone: (508) 820-2391

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: Cyr, Mark (POL)
To: Melander, John (EPS)
Cc: Staples, Jennifer (POL); Walczak, Ryan (POL); Pack, Noah (POL)
Subject: ALPR Policy - Updated June 27, 2023
Date: Thursday, September 21, 2023 9:53:23 AM
Attachments: TRF-11 Automatic License Plate Recognition (1).pdf

---

John,

Please find the department's current ALPR policy attached.

Mark

Lieutenant Colonel Mark D. Cyr #2728
Massachusetts State Police
Division Commander
Division of Homeland Security and Preparedness
508-988-7301 (office)
[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: Handfield, Kenneth (POL)
To: Snow, Corrine (POL); Dunbar, Cameron (POL); Demers, Joanne (POL); Ross, Jonathan (POL); Keville, Robert (POL); Gleason, Kristin (POL); Cheverie, Peter (POL); Quinn, Heather (POL); Teevens, Richard (POL); Dunphy, Thomas J (POL)
Subject: ALPR Policy & Use
Date: Tuesday, June 27, 2023 3:05:18 PM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

Sups,

Please make the attached policy known to your dispatchers. As it reads, the Commonwealth Watch Center and the Commonwealth Fusion Center are the primary ALPR resources for the Department; and any non-Department ALPR Systems accounts are prohibited unless approved by the Division Commander of Homeland Security and Preparedness, through your chain of command.

If your center or any of its personnel have Department ALPR and/or non-Department ALPR accounts, please let me know by end-of-week so a determination can be made about access and use.

Thank you,
Ken

Kenneth E. Handfield, Jr.
Director of Dispatch Services

Massachusetts State Police
Communications Section, Dispatch Services Unit
50 Maple Street, Rm. 2330
Milford, MA 01757

Office: 508.820.2347
Cell & Text: [redacted]

Fax: 774.462.3768 (Milford)

Email: Kenneth.Handfield@Mass.gov

From: Pack, Noah (POL)
To: Staples, Jennifer (POL); Brunelli, Daniel (POL); Cyr, Mark (POL)
Subject: ALPR Policy Draft
Date: Wednesday, March 1, 2023 1:46:23 PM
Attachments: TRF-11 Automatic License Plate Recognition DRAFT 16 3-1-23.docx

Attach is the latest draft of the revised ALPR policy 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: Pack, Noah (POL)
To: Staples, Jennifer (POL); Brunelli, Daniel (POL)
Cc: Cyr, Mark (POL)
Subject: ALPR Policy Review
Date: Wednesday, February 8, 2023 1:55:13 PM
Attachments: TRF-11 Automatic License Plate Recognition DRAFT 15.docx

Good afternoon Jenn and Dan,

As LTC Cyr mentioned, we would like to review the ALPR policy and discuss potential updates. The attached draft includes several modifications and ideas for discussion, and its fair to say that they will need to be changed or removed based upon our discussion and your advice.

Once you've had time to review, would you be willing to meet to discuss before the EOPSS call on 2/21?

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: Cyr, Mark (POL)
Subject: ALPR Policy Revision Draft
Date: Monday, May 1, 2023 5:02:27 PM
Attachments: TRF-11 Automatic License Plate Recognition DRAFT 2023.docx
TRF-11 Nov21.pdf

LTC Cyr:

Cleaned-up and most recent draft is attached, along with a copy of the general order currently in effect.

Respectfully,

Noah

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

From: Cyr, Mark (POL)
To: Condlin, Christopher (POL)
Cc: Powers, Liam (POL); Pack, Noah (POL)
Subject: ALPR Policy Revision Draft
Date: Friday, May 5, 2023 1:51:46 PM
Attachments: TRF-11 Automatic License Plate Recognition DRAFT 2023 (1).docx

---

Good afternoon Chris,
Please find attached the ALPR policy revision draft. I believe it will need some formatting. If possible, can we include it in this quarter's batch awaiting promulgation? Legal has already reviewed and approved. Please do not hesitate to reach out with any questions/concerns.

Thank you,
Mark

Lieutenant Colonel Mark D. Cyr #2728
Massachusetts State Police
Division Commander
Division of Homeland Security and Preparedness
508-988-7301 (office)
[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)
To: Pack, Noah (POL)
Subject: ALPR Policy Update
Date: Saturday, July 1, 2023 9:07:37 PM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

Notification of ALPR Policy Update

The Department's ALPR policy (TRF-11) was officially updated as of June 27, 2023. An updated copy is attached to this email. This policy governs the use of the ALPR systems by sworn and civilian members of MSP. Please review it to ensure you are familiar with the most recent version. Many of the updates directly reflect the best practices that we have already been using and teaching, such as limiting the scope of searches and the duration of manual hotlist entries.

One noteworthy update is that a manual hotlist entry request must be authorized by a supervisor, except in exigent circumstances/emergencies. This can be satisfied in one of two ways: (1) the request can come directly from a supervisor (Sgt. or above or civilian equivalent), or (2) the requestor can provide the name of the supervisor who has authorized the request. If you or a member of your unit submits a hotlist request to the Watch Center, they will respond with an inquiry about this authorization if it does not meet one of those criteria in the initial request.

As always please feel free to reach out with questions, comments, or success stories.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

From: Staples, Jennifer (POL)
To: Brunelli, Daniel (POL)
Subject: ALPR Policy
Date: Monday, April 10, 2023 11:56:33 AM
Attachments: image001.png
TRF-11 Automatic License Plate Recognition DRAFT 19 3-13-23.Legal.Edits.4.10.23.docx

---

Hey Dan:

I made some tweaks that I think addresses our concerns and Pack's concerns.

Let me know your thoughts.

Jennifer M. Staples
Chief Legal Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Tel: (508) 820-2307
Cell: [redacted] G.L. c. 4.sec. 7.cl.26 (n)(security)

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: Melander, John (EPS)
To: Pack, Noah (POL)
Subject: ALPR Policy
Date: Thursday, October 12, 2023 2:42:13 PM
Attachments: TRF-11 Automatic License Plate Recognition (1).pdf

---

Hi Noah,

Could you tell me what part of the attached policy was added/amended in June? I think the “Use of Non-Departmental ALPR System” was added, so just wondering if anything else changed in June. Maybe you have a redline?

Thanks!

John Melander
Deputy General Counsel
Executive Office of Public Safety and Security
One Ashburton Place, Suite 2133
Boston, MA 02108
Cell: [redacted] G.L. c. 4 sec. 7 cl.26 (n)(security)

From: Cyr, Mark (POL)
To: Kwon, Gina K. (EPS)
Subject: ALPR Revised Policy DRAFT and Current ALPR Policy
Date: Monday, May 1, 2023 5:40:23 PM
Attachments: TRF-11 Nov21.pdf
TRF-11 Automatic License Plate Recognition DRAFT 2023.docx

U/S,
As requested, please find attached the revised ALPR policy draft and our current ALPR policy. We hope to promulgate the revised version soon. Please don't hesitate to reach out with any questions or concerns.

Thank you,
Mark

Lieutenant Colonel Mark D. Cyr #2728
Massachusetts State Police
Division Commander
Division of Homeland Security and Preparedness
508-988-7301 (office)
G.L. c. 4,sec. 7,cl.26 (n)(security) *(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: Walczak, Ryan (POL)
To: Mcnamara, Sean (POL)
Subject: ALPR Slides
Date: Tuesday, September 19, 2023 11:08:17 AM
Attachments: LPR Training Powerpoint.pdf

See attached.

Respectfully,

Sergeant Ryan Walczak #3731
Massachusetts State Police
Division Of Homeland Security and Preparedness
Technical Services Unit
Cell #[redacted] M.G.L. c. 4,sec. 7,cl.26 (n)(security)
Email: Ryan.walczak@pol.state.ma.us

From: Pack, Noah (POL)
To: Pack, Noah (POL)
Cc: Walczak, Ryan (POL)
Subject: ALPR Update Materials
Date: Tuesday, August 8, 2023 2:49:30 PM
Attachments: Neology PAGIS-2.15 User training.pdf
TRF-11 Automatic License Plate Recognition.pdf

Hello all:

Our records indicate that you are currently assigned to a DFS cruiser that has an ALPR system on it. That system is *NOT* currently in service (meaning working and allowed to connect to and receive alerts/hits). We are hopeful that funding will become available to conduct the necessary updates and/or maintenance to your device, and we hope to get your systems online in the reasonably near future.

In preparation, please review the attached training materials. For those who have not previously received it, a familiarization training either in-person or via remote meeting/call will also be provided.

You are required to review these materials prior to having the ALPR systems on your cruisers activated or re-activated:

1. General Order TRF-11, the Department's ALPR policy
2. Neology PAGIS 2.15 User Training, a pdf document

Please reply to this message, including Sergeant Ryan Walczak of the Technical Services Unit, indicating when you have reviewed the materials and if you understand them or have any questions.

Respectfully,

Sergeant Noah H. Pack
Massachusetts State Police

From: Lorenco, Nicholas (POL)
To: Kory Koster
Subject: ALPR Updated list
Date: Tuesday, May 9, 2023 8:54:41 AM
Attachments: ALPR CRUISER LIST (UPDATED).pdf
Outlook-baw3qgzw.png

ALPR CRUISER LIST (UPDATED).xlsx

Trooper Nicholas Lorenco #4165
Massachusetts State Police
Troop-S, Special Operations
Commercial Vehicle Enforcement Section
906 Elm Street
Concord, MA 01742
Section Office: (978) 369-1004
Google Voice: (857)-574-0030
Fax (978) 369-5353
E-Mail: Nicholas.Lorenco@pol.state.ma.us

From: Stelmat, Jason (POL)
To: Smith, Eleanor (POL)
Subject: ALPR
Date: Thursday, February 9, 2023 12:13:00 PM
Attachments: TRF-11 Automatic License Plate Recognition.pdf
image001.png

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

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. Thank-you.

Please consider the environment before printing this e-mail

From: Tucker, Daniel T (POL)
To: Kwon, Gina K. (EPS); Cyr, Mark (POL)
Subject: ALPR
Date: Thursday, August 17, 2023 9:47:35 AM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

Good morning,

As requested, I have attached information on Automatic License Plate Readers to this email.

Thank you,
Dan

Major Daniel T Tucker #2938
Massachusetts State Police
Division of Homeland Security and Preparedness
Deputy Division Commander - CIIS
(office) 978-451-3754
(cell) [redacted] M.G.L. c. 4,sec. 7.cl.26 (n)(security)

From: John Tedona
To: Pack, Noah (POL)
Cc: Bradley Feldmann; Luke Normington; mroth
Subject: BOSS / PAGIS Status Summary
Date: Friday, February 10, 2023 1:13:21 PM
Attachments: image001.png
image002.png
image003.png
MSP Status Report - Feb 10.pdf

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

Noah,

I've attached the current status report slide deck that captures are reported bugs and planned features for your review. As shown in the slide deck we've made some significant progress in correcting bugs attributed to the overall system software, mobile hardware and GPS coordinate problem.

Highlights are:

- All bugs referenced on slide #3 in RC 58 and RC 59 are in their last steps in QA and are all scheduled to be released to BOSS4 v59 on March 6th

- PAGIS bugs referenced on slide #6, excluding the GPS coordinate issue, have gone through QA and have been corrected in PAGIS 2.15.2.12 All PAGIS bugs including the GPS coordinate issue will be corrected in PAGIS version 2.15.2.13 and will be released on Fed 27th.

- Reported issues where the SX4e processor seems to be functioning (lights on but not booting to PAGIS application) we have been able to a) replicate this and b) partially identify the cause. This is caused by a Windows10 "write-lock" feature which is enabled on the processor units. This write-lock is purposefully used, and has been in previous generations of SX4/SX3 generations to protect the configuration of the processor and its Operating System. In VP-relay mode, as is used by MSP (and others), this write lock has been replicated to show that in roughly 0.5% of restart/reboot cases that the Operating System will hang, meaning that PAGIS never gets to a boot status. Hence the reporting status that the processor seems to be working (lights on etc) but not being able to see Pagis. The work-around at the moment is a power-cycle when this happens which in all tested cases seems to clear the problem. In one situation the team had to power cycle the unit 3 times before it cleared however in every other case, a single power cycle resolved the lock. The engineering team at manufacturing are working through the configuration to better understand and identify what is causing this so we are able to provide a script to update the config to resolve this.

Thanks,

John Tedona
Sales Manager

Mobile: [redacted]
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
https://www.policegrantshelp.com/neology-grant-assistance/ - Grant Assistance

From: John Tedona
To: Pack, Noah (POL)
Cc: Bradley Feldmann; mroth; Luke Normington; Giovanni Navarrete Araiza
Subject: BOSS/PAGIS Status Summary
Date: Wednesday, February 22, 2023 5:04:11 PM
Attachments: image001.png
image002.png
image003.png
MSP Status Report_2222023.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 Noah,

I've attached the latest status report slide deck that outlines resolved & open bugs and planned feature updates for your review.

Highlights are:

- As indicated on slide #3 RC 59 has been incorporated into and RC 58 and are in their last steps in QA and are scheduled to be released on March 6th.
- PAGIS (update) referenced on slide #6, eleven PAGIS issues have been resolved; however further Q&A testing uncovered four previously unknown issues. Recommendation is to delay the PAGIS software version two weeks (February 27th to March 13th) to ensure all issues are resolved.

Please let me know if I can provide any additional information.

Thanks,

John Tedona
Sales Manager

Mobile: [redacted]
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
https://www.policegrantshelp.com/neology-grant-assistance/ - Grant Assistance

From: John Tedona
To: Pack, Noah (POL)
Cc: Bradley Feldmann; mroth; Luke Normington; Giovanni Navarrete Araiza; Israel Padilla Sanchez
Subject: BOSS/PAGIS Status Summary
Date: Monday, March 6, 2023 3:33:09 PM
Attachments: image001.png
image002.png
image003.png
MSP Status Report_362023.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 Noah,

I've attached the latest status report slide deck that outlines resolved & open bugs and planned feature updates for your review.

The Development team is in the process of preparing the software for deployment on the MSP Production instance for Wednesday night. Israel will contact you to go over the update logistics.

Please let me know if I can provide any further information.

Thanks,

John Tedona
Sales Manager

Mobile: [redacted]
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
https://www.policegrantshelp.com/neology-grant-assistance/ - Grant Assistance

From:	Israel Padilla Sánchez
To:	Pack, Noah (POL)
Cc:	Giovanni Navarrete Araiza; John Tedona; mroth; Michell Itallekzi Garcia Garcia; Daniela Geraldine Ponce Calderon
Subject:	BOSS4 v59 - Release Notes
Date:	Tuesday, May 9, 2023 12:58:30 AM
Attachments:	Outlook-Logo Desc.png Outlook-signature .png Outlook-signature .png BOSS4 v59 - Release notes.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 Sergeant,

Please find attached to this e-mail the release notes for BOSS4 version 59. If you agree, we could perform the upgrade process tomorrow (Tuesday, May 9th) during the night. The update process should take less than 1 hour.

Let us know if we can proceed.

Best regards

--

Israel Padilla Sánchez
Solutions Delivery Manager

Mobile: +[redacted]
Email: ipadilla@neology.mx

Lago Zúrich 219 Office 1001
Mexico City, CDMX 11529

www.neology.net

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

From: Kevin Haskins
To: Fitzgerald, Carol (POL)
Subject: Chorus Intelligence and MASP
Date: Monday, March 13, 2023 12:04:04 PM
Attachments: image001.png
CIS Brochure 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.

Hi Carol,

We are rolling out our technology to the NH State Police and NH Attorney General's Office and I would like to see if you and your team would consider giving our intelligence platform a trial. There is no financial outlay or commitment to purchase. I would only ask for your honest feedback. I am local to you and would be happy to provide an in-house demonstration for you and your team at your convenience. I have attached our product brochure for your review, consideration, reference, and distribution as needed. I would only need about an hour of time. Please let me know what your schedule permits.
Best,

Kevin HASKINS
Chorus Intelligence
Business Development Director
C: 781.929.8843
E: k.haskins@chorusintel.com
www.chorusintel.com/us

Chorus
Discover • Link • Solve

Making the world a safer place

This email and any files transmitted with it are confidential and intended solely for the addressee.
The information contained in this electronic message is intended only for the above named recipient and may be privileged or confidential.
They may contain information that is covered by legal, professional or other privilege.
Chorus Intelligence Ltd. Reg. Office: 6 Quay Point, Station Road, Woodbridge, IP12 4AL. Reg. in England and Wales No. 07814100. Vat Reg No. 124331259
Chorus Intelligence Inc, Reg. Office: 4525 Main Street, Suite 710, Virginia Beach, VA 25462

From: Fafard, Matthew (POL)
To: Weldon, Stephen (POL)
Subject: CJIS Audit of GHQ
Date: Wednesday, August 9, 2023 11:23:49 AM
Attachments: 0 - CJIS 2021-2024 AUDIT GUIDE.docx

Steve,

DCJIS has asked that we explain and provide documentation to demonstrate compliance with CJIS IT requirements. Please take a look at the Information Technology section in the attached Audit Guide document and let me know what we have for answers/documentation for them. They are auditing GHQ on August 22. Thanks

Captain Matthew R. Fafard
Massachusetts State Police
Division of Administrative Services
470 Worcester Road, Framingham, MA 01702
Office: 508-820-2107
matthew.fafard@pol.state.ma.us

From:	Lazar, Ellyn (MID)
To:	Macdonald, Michael (POL)
Subject:	Court Decision - Commonwealth v. Jerron Perry (Cell Towers, Search & Seizure, Expectation of Privacy) - April 1, 2022
Date:	Tuesday, January 24, 2023 2:56:10 PM
Attachments:	image001.png Tower dumps-Perry.rtf

From: Stone, Jessica (DAA) <Jessica.Stone@mass.gov>
Sent: Friday, April 1, 2022 11:33 AM
To: DAA-DL-DA&EXEC.ASST <DAA-DL-DA&EXEC.ASST@MassMail.State.MA.US>; DAA-DL-ADA's <DAA-DL-ADA's@MassMail.State.MA.US>; DAA-DL-Case Summaries <DAA-DL-CaseSummaries@MassMail.State.MA.US>
Subject: Court Decision - Commonwealth v. Jerron Perry (Cell Towers, Search & Seizure, Expectation of Privacy) - April 1, 2022

SUPPORTING MASSACHUSETTS PROSECUTORS
MDAA
Massachusetts District Attorneys Association

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:	Ryan Barnett
To:	sam.rabadi@motorolasolutions.com; Pack, Noah (POL); JAMES DOWLING; lisa.benincasa@motorolasolutions.com
Cc:	Ally Yoegel; Tom Joyce; Ryan Barnett
Subject:	Covert Discussion Follow-up
Date:	Friday, January 20, 2023 10:09:02 AM
Attachments:	VSS22-CovertEnclosures-072822-DIGITAL.pdf VSS-VVT-Digital-111821.pdf VSS22-VettedVirtualTechnicianRS (1).pdf Vetted Security Solutions Warranty Statement_Enclosures.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 All,

I very much appreciate the time this week discussing our covert solution. Attached is the spec sheet on the two solutions and photos of the two enclosure types we are quoting. The two enclosures are turnkey with all optics, processors, and can be preconfigured to your LEARN account and setup for cellular if you provide your SIM card to us ahead of equipment shipping.

We expect lead time between 30-45 days from time the order is placed. There are no minimums unless there are requested changes to enclosure types or a new enclosure design. All enclosures come with a 1 year hardware manufactures warranty, the warranty statement is attached as well for your reference.

Please do not hesitate to let us know if you have any questions and our team will get the quote around to you shortly.

Thanks,

Ryan Barnett
Chief Executive Officer
Vetted Holdings
C: 727-793-1215
O: 727-440-3245
LinkedIn: linkedin.com/ryan
https://vettedholdingsllc.com/

From: Ayers, Kathleen
To: Brunelli, Daniel (POL)
Cc: Hynes, Allison E (POL)
Subject: CT challenges to LPR cameras
Date: Tuesday, February 7, 2023 11:43:37 AM
Attachments: New Haven Register Article Dec 2022.pdf
AUTOMATIC LICENSE PLATE RECOGNITION SYSTEMS.pdf
A&O 13.16.2 LPRs.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.

Dear Dan

I did some quick looking this morning and I did not find any court challenges to CT police's use of license plate reader cameras. The ACLU has been vocal about their concerns re: privacy and retention, but the one bill proposed in 2012 that would have limited retention to 2 weeks did not pass the House.

Also, I couldn't find the 5-year retention period that my colleague referred to yesterday. Instead, I see that our own State Police A&O Manual policy lists retention at 90 days unless the footage is tagged as evidence. That is the same policy we use for all our camera footage.

I attached to this email some more materials that might be helpful. The newspaper article contains a link to a 2019 ACLU report that is over 1,000 pages; it may provide a glimpse into any potential challenges.

Please let me know what else I could look into to help you all with this.

Thank you,

Kate Ayers
Staff Attorney 2
Department of Emergency Services and Public Protection
Phone: (860)-685-8150
Fax: (860)-685-8611
kathleen.ayers@ct.gov

NOTICE: This e-mail transmission and any accompanying attachments may contain confidential or privileged information. They are intended for use by the individual or entity named on this e-mail transmission. If you are not the intended recipient, you are not authorized to disclose, copy, distribute or use, in any manner, the contents of this information. If you have received this e-mail transmission in error, please notify us by e-mail immediately.

From: Levine, Doug (POL)
To: Mackey, Corey (POL)
Cc: Procopio, David (POL)
Subject: DHS report edit suggestions
Date: Monday, June 5, 2023 3:05:22 PM
Attachments: 2022 DHS Annual Report (5JUN23) DL comments.docx

---

Hey Corey,

Attached please find the DHS annual report section with my suggested cuts (contained in comments in the margins).

Please work your magic to further reduce the section so it doesn't end up being much more than 12 to 14 pages or so (the 2019 Annual Report contained 17 pages for DHS, and the 2021 report contained 8 pages). I also don't want cut language/information that you think is critical to keep.

I appreciate your help.

My best,
Doug

Doug Levine
Special Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
(508) 820-2394 | Office
[redacted] | Mobile

To:	Unit Commanders - DHS
Cc:	Cyr, Mark (POL); Tucker, Daniel T (POL); Rudolph, James (POL); Grasso, Jimi (POL); Nunes, John (POL); Concannon, James (POL); Miskell, Michael (POL); Connors, Brian (POL); Pagliaroni, Anthony (POL); Barton, Shannan F. (POL); Palmer, David (POL); McGonagle, Mary (POL); Small, Michelle (POL); Gabriel, Stephen (POL); Wolf, Amy (POL); Howard, Michael HR/MSP (POL); Vasapolli, Jennifer (POL); Rivera Morgan, Awilda (POL); Mills, Melissa (POL); Pinkham, John (POL); Diotte, Jeffrey (POL); Wheeler, Mark (POL); Richard, Daniel (POL); Prokopovich, Jenny L. (POL); Mawn, John (POL); Sullivan, Kristen (POL); Place, Cassandra (POL); Morris, Samantha (POL); Staples, Jennifer (POL); Kelly, Siobhan (POL)
Subject:	Division Commander"s Order 2023-DHS-015
Date:	Wednesday, September 13, 2023 6:09:53 PM
Attachments:	DC Order 2023-DHS-015 ALPR Data Retention and Access.pdf

Good Afternoon,

Attached, please find Division Commander's Order 2023-DHS-015. This Order has also been posted to PowerDMS.

Please ensure all those under your command are aware of this Order.

Respectfully,

Rose

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

From:	Warren, Rosemary (POL)
To:	Aumais, Matthew (POL); Banik, John (POL); Barry, Sean (POL); Bellao, Shaun (POL); Boyle, Christopher (DOT); Boyle, Christopher (POL); Brooks, Brian (POL); Bruce, James (POL); Cerra, Robert (POL); Conron, John (POL); Czepiel, Ryan (POL); Deas, James (POL); Dorian, Christine (POL); Fairchild, Eric (POL); Gavioli, Brian (POL); George, Michael (POL); Josti, Michael (POL); Kardoos, Albert (POL); Kaupp, Kevin (POL); Mahoney, Brian (POL); Mccarron, Richard (POL); McLaughlin, Kelly (POL); Nason, Nicholas (POL); O"Hara, Edward (POL); OToole, Kevin (POL); Pack, Noah (POL); Perry, Jeffrey (POL); Popovich, Andrew D (POL); Quigley, Robert (POL); Quirk, Sean (POL); Racki, Steven M (POL); Riley, Patricia (POL); Shink, Norman (POL); Smith, Eleanor (POL); Strazzullo, John (POL); Telford, Erik (POL); Thibault, Amy (POL); Walsh, Mark (POL); Warren, Rosemary (POL)
Cc:	Cyr, Mark (POL); Tucker, Daniel T (POL); Rudolph, James (POL); Grasso, Jimi (POL); Nunes, John (POL); Concannon, James (POL); Miskell, Michael (POL); Connors, Brian (POL); Pagliaroni, Anthony (POL); Barton, Shannan F. (POL); Palmer, David (POL); McGonagle, Mary (POL); Small, Michelle (POL); Gabriel, Stephen (POL); Wolf, Amy (POL); Howard, Michael HR/MSP (POL); Vasapolli, Jennifer (POL); Rivera Morgan, Awilda (POL); Mills, Melissa (POL); Pinkham, John (POL); Diotte, Jeffrey (POL); Wheeler, Mark (POL); Richard, Daniel (POL); Prokopovich, Jenny L. (POL); Mawn, John (POL); Sullivan, Kristen (POL); Place, Cassandra (POL); Morris, Samantha (POL); Staples, Jennifer (POL); Kelly, Siobhan (POL)
Subject:	Division Commander"s Order 2023-DHS-015
Date:	Wednesday, September 13, 2023 6:11:24 PM
Attachments:	DC Order 2023-DHS-015 ALPR Data Retention and Access.pdf

Good Afternoon,

Attached, please find Division Commander's Order 2023-DHS-015. This Order has also been posted to PowerDMS.

Please ensure all those under your command are aware of this Order.

Respectfully,

Rose

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

From: Cyr, Mark (POL)
To: Warren, Rosemary (POL)
Subject: Divison Commander Order - ALPR
Date: Wednesday, September 13, 2023 12:35:47 PM
Attachments: ALPR Div Comm Order.docx

Lieutenant Colonel Mark D. Cyr #2728
Massachusetts State Police
Division Commander
Division of Homeland Security and Preparedness
508-988-7301 (office)
G.L. c. 4.sec. 7.cl.26 (n)(security) *(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: Thibault, Amy (POL)
To: Thibault, Amy (POL)
Subject: docs
Date: Thursday, July 20, 2023 10:20:20 AM
Attachments: CIIS Responsibilities AMY DRAFT March 4.docx
Macrimenet request for additional analyst.docx
MCP Duties and Responsibilities - Vacancies 2021.docx
Fusion Center Overview Academy 2021 (1).pptx

Respectfully,

Amy Thibault
Intelligence Services Manager
MA State Police
Intelligence Services Unit
Commonwealth Fusion Center
Main Number: 508-820-2233
Desk: 978-451-3717
amy.thibault@pol.state.ma.us

From: Pack, Noah (POL)
To: Grasso, Jimi (POL)
Subject: DOT Notes
Date: Wednesday, November 1, 2023 11:16:20 AM
Attachments: MSP DHS DOT Collocation Request 7-23 Notes Update3.doc

---

Major,

Here is a summary of the DOT request. LTC has a doc very similar to this from the latest contact attempt in July. If you don't see anything here that you are looking for, please advise.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Investigative Services
Critical Incident Technical Investigations (CITI)

From: Pack, Noah (POL)
To: Cyr, Mark (POL)
Subject: DOT Request
Date: Wednesday, July 5, 2023 1:41:06 PM
Attachments: MSP DHS DOT Collocation Request 10-2022 Letterheard.doc
MSP DHS DOT Collocation Request 7-23 Notes Update.doc

LTC:

Attached is the letter you sent to Foti last October.

Also attached is a summary with history and bullet points that may be helpful in your attempts to move this forward.

Respectfully,

Noah

From: Pack, Noah (POL)
To: Cyr, Mark (POL)
Subject: Draft MOU Request
Date: Friday, April 14, 2023 4:15:07 PM
Attachments: TFL FLock MOUs April23.docx

LTC, please see attached draft for your review.

Respectfully,

Noah

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

From: Ben Miller
To: Bernstein, Eric (POL)
Subject: Elsag ALPR / Mass State Police ; Presentation
Date: Friday, April 14, 2023 11:39:06 AM
Attachments: Presentation Elsag ALPR 2023 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.

Hello Lieutenant,

As a follow up to the email below, please find attached presentation which gives you an overview of our Company, Technology and Clients.

ELSAG ALPR provides significant benefits to Police in support of their missions :

- Largest share in USA ALPR industry to Law Enforcement specific deployments serving over 3000 agencies in all 50 States.
- Federal Agencies : Only ALPR supplier to be trusted by all branches of the US Federal Government (including FBI, HIDTA, DEA, Secret Service, US Army, US Navy, US Marines, etc.)
- On site or 24/7 remote customer support (with facilities in Greensboro NC and Brewster NY … next to Danbury CT less than 2 hours drive from Mass)
- Highest quality in industry, Built Cop Tough with many systems +10 years deployed and still operating.

I look forward to speaking with you at your convenience.

Best Regards, Ben

From: Ben Miller <ben.miller@leonardocompany-us.com>
Sent: Friday, April 14, 2023 11:27 AM
To: eric.bernstein@state.ma.us
Subject: Mass Chiefs ; Elsag ALPR / Mass State Police ; MPH M7 spec sheet

Hello Lieutenant,

It was a pleasure to speak with you at the Massachusetts Chiefs Show on Wednesday. As discussed, we would be pleased to offer our technology and customer service to improve your ALPR deployments.

Since your main interest is Mobile ALPR for your cruisers, please find attached a copy of our MPH (Mobile Plate Hunter) M7 (7th generation) Mobile ALPR system for your review.

I will send a follow up email which gives you an overview of our company plus our role in and dedication towards ALPR for Law Enforcement and look forward to speaking with you again at your

earliest convenience.

Best Regards, Ben

Ben Miller
Operations Director New England
Selex ES Inc., a Leonardo Company
ELSAG® ALPR Plate Recognition Technology
Proudly Made in the USA
4221 Tudor Lane
Greensboro, North Carolina 27410 USA
ben.miller@leonardocompany-us.com
Cell: +1 [redacted]
www.elsag.com

The content of this email is confidential and intended for the recipient specified in message only. It is strictly forbidden to share any part of this message with any third party, without a written consent of the sender. If you received this message by mistake, please reply to this message and follow with its deletion, so that we can ensure such a mistake does not occur in the future.

From: Comeau, Melissa (POL)
To: Pack, Noah (POL)
Subject: FFY20 AHTF GAM updated
Date: Tuesday, September 5, 2023 3:41:39 PM
Attachments: 2020 COPS AHTF GAM Aug 2023 with edits KH-JL-MC.docx

---

Here is last week's version….

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: Henry, Karen E. (POL)
Subject: FFY20 AHTF modification
Date: Thursday, August 10, 2023 1:57:00 PM
Attachments: 2020 COPS AHTF GAM July 2023.docx

I am hoping to shorten this….
Tell me if you agree.

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: Toto, John (FMCSA)
To: Noe, Vincent (POL)
Subject: Final for review
Date: Thursday, March 16, 2023 2:14:42 PM
Attachments: image001.png
image002.png
Finial MCSAP Qualifying Conditions Review Checklist revision State Filled FINAL.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.

John Toto, State Programs Specialist/Special Agent
Massachusetts Division
Federal Motor Carrier Safety Administration
50 Mall Rd., Suite 212, Burlington, MA 01803
P: (781) 425-3212 | F: (781) 425-3225 | M: (857) 292-3122
john.toto@dot.gov

U.S. Department of Transportation
Federal Motor Carrier Safety Administration

*This FMCSA Special Agent is duly accredited by the Secretary of Transportation with the authority to enter upon, inspect, and examine lands, buildings, and equipment, and to inspect and copy records and papers of carriers and other persons, in performance of his/her duties under the Department of Transportation Act, related acts, and regulations of the Department.

From: Sullivan, John (POL)
To: Connors, Brian (POL); Cyr, Mark (POL); Farley, Michael (POL); Benson, Eric (POL)
Cc: Banik, John (POL)
Subject: Flock ALPR_VFAS
Date: Friday, August 4, 2023 1:16:25 PM
Attachments: Flock_To_From.doc

Please see attached To/From. Respectfully,

Sully

Detective Lieutenant John B. Sullivan #3359
Massachusetts State Police
Unit Commander
Violent Fugitive Apprehension Section
Office: 508-820-2374
Cell: [redacted]

From: Sullivan, John (POL)
To: Foley, Kristine (POL)
Subject: Flock
Date: Friday, October 6, 2023 10:43:13 AM
Attachments: Flock_To_From.doc

Detective Lieutenant John B. Sullivan #3359
Massachusetts State Police
Unit Commander
Violent Fugitive Apprehension Section
Office: 508-820-2374
Cell: [redacted]

Subject: FW: 2020HPWX0004 GAM
Date: Monday, November 20, 2023 3:46:50 PM
Attachments: 2020 COPS AHTF GAM Oct 2023 FINAL.docx

Subject: FW: 2020HPWX0004 GAM
Date: Tuesday, November 14, 2023 9:04:32 AM
Attachments: 2020 COPS AHTF GAM Oct 2023 FINAL.docx

From: Rust, Rebecca (POL)
To: Benton, LaShawn (COPS)
Cc: Comeau, Melissa (POL); Ly, Jeff (POL)
Subject: FW: 2020HPWX0004 GAM
Date: Monday, November 20, 2023 3:47:00 PM
Attachments: 2020 COPS AHTF GAM Oct 2023 FINAL.docx

Hi LaShawn:
I would just like to follow up on the below question. Our GAM included a request to increase the equipment line for pursuit mitigation equipment. These are covert tracking devices that also require a subscription, which would be categorized as "other". The cost for this one year of airtime and access to CovertTracking mapping is $1,620. Would this subscription be allowable under this GAM? If allowable, would the entire year's cost be allowable, or would we have to prorate the cost to align with the end date of the grant (06/30/2024)?

Thanks,

Rebecca Rust
Deputy Director of Grants and Special Projects
Massachusetts State Police
470 Worcester Road
Framingham, MA 01712
508-820-2688
Rebecca.Rust@pol.state.ma.us

Your feedback is important to us. We value your input to continuously improve and provide you with the best possible service.
Please let us know how we are doing by taking our short survey at the following link:
MSP Crime Laboratory Service Satisfaction Survey

All communications sent or received by this Commonwealth of Massachusetts email address may be subject to disclosure under the Massachusetts Public Records Law (M.G.L. Chapter 66, Section 10) and the Federal Freedom of Information Act.
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: Rust, Rebecca (POL)
Sent: Wednesday, November 8, 2023 5:03 PM
To: Benton, LaShawn (COPS) <LaShawn.Benton2@usdoj.gov>
Cc: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>; Ly, Jeff (POL) <Jeff.Ly@pol.state.ma.us>
Subject: RE: 2020HPWX0004 GAM

Good afternoon:
The attached GAM was recently approved. We appreciate such a quick turnaround time!

We have one additional question. Our GAM included a request to increase the equipment line for pursuit mitigation equipment. These are covert tracking devices that also require a subscription, which would be categorized as "other". The cost for this one year of airtime and access to CovertTracking mapping is $1,620. Would this subscription be allowable under this GAM? If allowable, would the entire year's cost be allowable or would we have to prorate the cost to align with the end date of the grant (06/30/2024)?

Thank you!

Rebecca Rust
Deputy Director of Grants and Special Projects
Massachusetts State Police
470 Worcester Road
Framingham, MA 01712
508-820-2688
Rebecca.Rust@pol.state.ma.us

Your feedback is important to us. We value your input to continuously improve and provide you with the best possible service.
Please let us know how we are doing by taking our short survey at the following link:
MSP Crime Laboratory Service Satisfaction Survey

All communications sent or received by this Commonwealth of Massachusetts email address may be subject to disclosure under the Massachusetts Public Records Law (M.G.L. Chapter 66, Section 10) and the Federal Freedom of Information Act.
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: Benton, LaShawn (COPS) <LaShawn.Benton2@usdoj.gov>
Sent: Wednesday, October 18, 2023 5:25 PM
To: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Cc: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>; Ly, Jeff (POL) <Jeff.Ly@pol.state.ma.us>
Subject: RE: 2020HPWX0004 GAM

CAUTION: This email originated from a sender outside of the 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,

Thanks for the notice. I will review ASAP and let you know if I have questions or concerns.

Thanks

LaShawn Benton
Grants Management Specialist
Community Oriented Policing Services (COPS)
U.S Department of Justice
Email:lashawn.benton2@usdoj.gov

From: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Sent: Wednesday, October 18, 2023 1:14 PM
To: Benton, LaShawn (COPS) <LaShawn.Benton2@usdoj.gov>
Cc: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>; Ly, Jeff (POL) <Jeff.Ly@pol.state.ma.us>
Subject: [EXTERNAL] 2020HPWX0004 GAM

Good afternoon:
We just submitted a GAM in just grants for 2020HPWX0004, Anti-Heroin Task Force 2020. I have attached the letter that was attached. My apologies, our prior grant manager was Judith Williford,

and the documentation in Just Grants is addressed to her. Let us know if there is anything else you need to get this moving. We are available to answer any questions you my have.

Thanks so much!

Rebecca Rust
Deputy Director of Grants and Special Projects
Massachusetts State Police
470 Worcester Road
Framingham, MA 01712
508-820-2688
Rebecca.Rust@pol.state.ma.us

Your feedback is important to us. We value your input to continuously improve and provide you with the best possible service.
Please let us know how we are doing by taking our short survey at the following link:
MSP Crime Laboratory Service Satisfaction Survey

All communications sent or received by this Commonwealth of Massachusetts email address may be subject to disclosure under the Massachusetts Public Records Law (M.G.L. Chapter 66, Section 10) and the Federal Freedom of Information Act.
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: Bender, Sean (POL)
To: Thibault, Amy (POL)
Subject: Fw: 2022 Stats
Date: Tuesday, January 3, 2023 2:43:13 PM
Attachments: CFC Activity Report - 2022 FINAL.xlsx
CFC Significant Activity - Highlights - 2022.docx

Good Afternoon, Amy -

Please find the attached summary of CFC activity for 2022, as well as significant activity highlights from throughout the year.

2022

Requests for Information: 13,487

- **12,111 Requests for Database Checks**
- **239 "General Requests"**
- **3 Terrorist Screening Center Hits**
- **31 Interpol Requests**
- **1103 Requests for Technical Support (Coplink / ACISS)**

Database Check Request Breakdown:

- **State/Local Agencies: 11,212**
- **Federal Agencies: 538**
- **Other Fusion Centers: 290**
- **Other/Unclassified: 71**

Disseminations Breakdown:

- **CFC Internal Products: 687**
- **Federal Partner Products: 55**
- **State Partner Products: 25**
- **Local Partner Products: 139**
- **Other Fusion Center Products: 362**

SARs / Criminal Tips:

- **SARs Entered: 259**
- **SARs Forwarded to eGuardian: 214**
- **Criminal Tips: 586**

Respectfully,

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

From: George Michael (POL)
To: Walczak Ryan (POL)
Subject: FW: Airlink subscription renewal - TSU
Date: Thursday, August 3, 2023 2:21:34 PM
Attachments: image002.png
image003.png
image004.png
image005.png
image006.png
image007.png
image008.png
image009.png
image010.png
image011.png
image012.png
image013.png
image014.png
image015.png
image016.png
Airlink subscription quote.pdf

Modem support for alpr

From: Pearson, Gustav (POL) <Gustav.Pearson@pol.state.ma.us>
Sent: Thursday, August 3, 2023 9:46 AM
To: Pack, Noah (POL) <noah.pack@pol state.ma.us>
Cc: Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>; Doherty, Nancy (POL) <Nancy.Doherty@pol state.ma.us>; Walczak, Ryan (POL) <ryan.walczak@pol.state.ma.us>; George, Michael (POL) <Michael.George@pol state.ma.us>; Gray, Kellie (POL) <Kellie.Gray@pol.state.ma.us>; Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>; Biagi, Pamela (POL) <Pamela.Biagi@pol.state.ma.us>
Subject: RE: Airlink subscription renewal - TSU

Hi Noah

Thanks for reviewing this.

If the Budget Office agrees, I will await their funding approval for $4,816.23 and process the attached quote as a new PO.

Gustav Pearson
Accountant IV
Department of State Police
470 Worcester Road
Framingham, MA 01702
508 820-2128 ph
508 820-2165 fax
gustav.pearson@pol.state.ma.us

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Thursday, August 3, 2023 9:27 AM
To: Pearson, Gustav (POL) <Gustav.Pearson@pol state.ma.us>; George, Michael (POL) <Michael.George@pol.state.ma.us>; Gray, Kellie (POL) <Kellie.Gray@pol.state.ma.us>; Silva, Kyra (POL) <Kyra.Silva@pol state.ma.us>; Biagi, Pamela (POL) <Pamela.Biagi@pol state.ma.us>
Cc: Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>; Doherty, Nancy (POL) <Nancy.Doherty@pol.state.ma.us>; Walczak, Ryan (POL) <ryan.walczak@pol.state.ma.us>
Subject: Re: Airlink subscription renewal - TSU

Hi Gus,

Apologies for the delay getting back to you on this. Lieutenant Mike George and I discussed it yesterday.

We agree that this would be most efficiently done as a single invoice with an aligned expiration date, as you have it in that quote. The devices do not need to be split up; they will all fall under the DHS Technical Services Unit.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

From: Pearson, Gustav (POL) <Gustav.Pearson@pol.state.ma.us>
Sent: Friday, July 21, 2023 10:07 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>; George, Michael (POL) <Michael.George@pol.state.ma.us>; Gray, Kellie (POL) <Kellie.Gray@pol.state.ma.us>; Silva, Kyra (POL) <Kyra.Silva@pol state.ma.us>; Biagi, Pamela (POL) <Pamela.Biagi@pol state.ma.us>
Cc: Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>; Doherty, Nancy (POL) <Nancy.Doherty@pol.state.ma.us>
Subject: RE: Airlink subscription renewal - TSU

Hi all

As a follow-up, I spoke with Peg Sullivan about this service who thought it may make sense to combine the renewal for these devices into a single quote/renewal each year. The attached quote includes a common end date for all devices on 9/30/24, now that the vendor bills in fixed increments rather than their previous "token" system for monthly activations.

If it is appropriate to use a single funding source for these devices, I can enter this as a new OPAS request, and Peg can close out the below 3 renewals. I can add comments that the service is used by Homeland Security and TSU.

If the cost should be split up, the rep can do that too. (We would need to know how these devices are shared/split in order to request two (2) quotes from BCM)

Thanks

Gustav Pearson
Accountant IV
Department of State Police
470 Worcester Road
Framingham, MA 01702
508 820-2128 ph
508 820-2165 fax
gustav.pearson@pol.state.ma.us

From: Pearson, Gustav (POL)
Sent: Monday, July 17, 2023 11:09 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>; George, Michael (POL) <Michael.George@pol.state.ma.us>
Cc: Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>; Doherty, Nancy (POL) <Nancy.Doherty@pol.state.ma.us>; Gray, Kellie (POL) <Kellie.Gray@pol.state.ma.us>; Biagi, Pamela (POL) <Pamela.Biagi@pol.state.ma.us>; Silva, Kyra (POL) <Kyra.Silva@pol state.ma.us>
Subject: RE: Airlink subscription renewal - TSU

Hi Noah and Lt. George

The devices on this quote are combined from several previous PO's (TSU and Homeland Security).

Devices on quote:

10 - *AirLink Basic Remote Device Management (July 1, 2023 to Sept 30, 2024)*

123 - *AirLink Basic Remote Device Management (Oct 1, 2023 to Sept 30, 2024)*

1 - *AirLink Basic Remote Device Management (Nov 1, 2023 to Sept 30, 2024)*

5 - *AirLink Basic Remote Device Management (May 1, 2024 to Sept 30, 2024)*

Previous PO's / renewals in OPAS:

1.

Narrative Description Of Request	Request Number	
AirLink Device Mgmt Service (ALMS)	OTIS24 - 0028	1 Year - AirLink Device Management Service for Ninety-one (91) Devices 91

Shipping Instruction

Attn: Technical Services Unit - D-Lt. Crouse

FY23 8100-4443 3810 U10 $2,866 50

2.

Item Description	Mai
Sierra MP70 Router (w/Wifi)	17
Sierra Power Adapter	25
Sierra Cellular Antennas	34
AirLink Device Management Service (77 Devices)	1

Sierra routers/AirLink Mgmt (ALMS)	OTIS24 - 0029	
AirLink Device Management Service (77 Devices)	1	**Attn:** Brian Egnitz **Email:** brian.egnitz@state.ma.us **Phone:** 9784513710

FY22 8100-4443 3810 $3,660.00

3.

Item Description	Date
Sierra Wireless AirLink Basic Remove Device Management - 1 year subscription	60

AirLink Basic Remote Device Management subscription	OTIS24 - 0030

Attn

Noah Pack

FY23 8100-1001 7000 (unit 7000 not used with std. appropriation in FY24) $1,890.00

I spoke with Matt at BCM who explained that the renewals are complicated, because the quantities do not match exactly due to devices expiring and also Sierra's previous "token" system, etc. Matt says this quote, however, covers all devices referenced in the above past renewal orders (91+77+60)

*as a reminder the 91 above is not related to the 91 Airlink devices for the Coastal Camera Project and is just a coincidence

Because the maintenance for all devices are now combined on a single quote, I want to confirm the funding source with the Budget office before we process the PO. Do you know if this renewal cost should be under Homeland Security, the TSU, or perhaps split?

Thanks

Gustav Pearson
Accountant IV
Department of State Police
470 Worcester Road
Framingham, MA 01702
508 820-2128 ph
508 820-2165 fax
gustav.pearson@pol.state.ma.us

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>

Sent: Friday, June 30, 2023 11:30 AM
To: Pearson, Gustav (POL) <Gustav.Pearson@pol state.ma.us>
Cc: George, Michael (POL) <Michael.George@pol.state.ma.us>
Subject: Re: Airlink subscription renewal - TSU

Hi Gus,

That quote appears to be accurate in terms of number of devices and expiration dates. For what it's worth, we are already in a state of service interruption on those ten devices, but it's an administrative service so it's not the end of the world while this gets sorted out.

Respectfully,

Noah

From: Pearson, Gustav (POL) <Gustav.Pearson@pol.state.ma.us>
Sent: Friday, June 30, 2023 11:04 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: George, Michael (POL) <Michael.George@pol.state.ma.us>
Subject: RE: Airlink subscription renewal - TSU

Hi Noah

I wanted to follow up on this when you have a chance. It appears only 10 devices are up for renewal today – the rep did mention to me however that there will be no chance of service interruption, but I would like to have the renewal PO generated once you confirm the details on the quote.

Please let me know if you have any questions or if there is any info I can provide from past Airlink PO's etc.

Thanks

Gustav Pearson
Accountant IV
Department of State Police
470 Worcester Road
Framingham, MA 01702
508 820-2128 ph
508 820-2165 fax
gustav.pearson@pol.state.ma.us

From: Pearson, Gustav (POL)
Sent: Tuesday, June 27, 2023 5:40 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: George, Michael (POL) <Michael.George@pol.state.ma.us>
Subject: RE: Airlink subscription renewal - TSU

Noah

Great, thanks. If the dates look correct to you (below), do you how the subscription end date of 6/30/23 decreased down to only 10 devices expiring next week? Reference last year's PO for 60 devices which noted a 6/30/23 end date.

10 - *AirLink Basic Remote Device Management (July 1, 2023*

123 - *AirLink Basic Remote Device Management (Oct 1, 2023*

1 - *AirLink Basic Remote Device Management (Nov 1, 2023 to*

5 - *AirLink Basic Remote Device Management (May 1, 2024 to*

I spoke with BCM about this briefly and understand Sierra / Airlink used to use a “token” system to apply subscription credit to devices. The orders would generate a “pool” or “bank” of tokens and they could be applied to different devices as needed for 1 month each. Could this be how the subscription dates may have been shifted? I understand Sierra moved away from the token subscription format.

Thanks

Gustav Pearson
Accountant IV
Department of State Police
470 Worcester Road
Framingham, MA 01702
508 820-2128 ph
508 820-2165 fax
gustav.pearson@pol.state.ma.us

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Tuesday, June 27, 2023 5:29 PM
To: Pearson, Gustav (POL) <Gustav.Pearson@pol state.ma.us>
Cc: George, Michael (POL) <Michael.George@pol.state.ma.us>
Subject: RE: Airlink subscription renewal - TSU

Even better! I’ll confirm the numbers and get back to you soon.

Respectfully,

Noah

From: Pearson, Gustav (POL) <Gustav.Pearson@pol.state.ma.us>
Sent: Tuesday, June 27, 2023 4:37 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: George, Michael (POL) <Michael.George@pol.state.ma.us>
Subject: RE: Airlink subscription renewal - TSU

Hi Noah

I don’t believe annual request letters are required here as they are renewals, and the renewal POs are processed each year by EOPSS.

I will research the PO history but believe that is the case here similar to Software maintenance renewals. Also, many To/From letters will also request future, recurring annual support to be funded on an ongoing annual basis.

Thanks

Gustav Pearson
Accountant IV
Department of State Police
470 Worcester Road
Framingham, MA 01702
508 820-2128 ph
508 820-2165 fax
gustav.pearson@pol.state.ma.us

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Tuesday, June 27, 2023 4:33 PM
To: Pearson, Gustav (POL) <Gustav.Pearson@pol state.ma.us>; George, Michael (POL) <Michael.George@pol.state.ma.us>
Subject: RE: Airlink subscription renewal - TSU

Hi Gus,

I will check this against our account and confirm. I think the idea here is so that we (Lt. George will be writing for this one) only have to write this renewal request letter once a year. If you want to split them up into multiple quotes, we will still want to include them all in one request letter. Any issues with that approach?

Respectfully,

Noah

From: Pearson, Gustav (POL) <Gustav.Pearson@pol.state.ma.us>
Sent: Tuesday, June 27, 2023 4:24 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>; George, Michael (POL) <Michael.George@pol.state.ma.us>
Subject: RE: Airlink subscription renewal - TSU

Hi Noah

As you know, BCM generated the attached. Could you review for accuracy, and I can process the renewal PO for the devices which have a subscription ending on 6/30/23? (It appears to be 10 devices that are due for renewal)

I may need to have BCM split this up into multiple quotes, but it's a good idea to synchronize the end dates to be able to process them together for October 2024.

Thanks

Gustav Pearson
Accountant IV
Department of State Police
470 Worcester Road
Framingham, MA 01702
508 820-2128 ph
508 820-2165 fax
gustav.pearson@pol.state.ma.us

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Thursday, June 22, 2023 12:27 PM
To: George, Michael (POL) <Michael.George@pol state.ma.us>
Cc: Pearson, Gustav (POL) <Gustav.Pearson@pol.state.ma.us>
Subject: Re: Airlink subscription renewal - TSU

Got it. In light of that, would you like to combine those renewals into one to get them all on a single schedule/invoice? I'm happy to contact Matt at BCM to have him adjust these to one document.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702

From: George, Michael (POL) <Michael.George@pol.state.ma.us>
Sent: Thursday, June 22, 2023 9:22 AM
To: Pearson, Gustav (POL) <Gustav.Pearson@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Perry, Jeffrey (POL) <Jeffrey.Perry@pol.state.ma.us>
Subject: RE: Airlink subscription renewal - TSU

FYI Both these invoices are for existing and deployed Airlink modems.

The meeting we had yesterday on Coastal Camera Project cleared up this issue – the 91 airlink invoice is merely a coincidence with the exact amount of cameras ordered on the coastal project.

Sorry for the confusion.

From: Pearson, Gustav (POL) <Gustav.Pearson@pol.state.ma.us>
Sent: Thursday, June 22, 2023 9:09 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: George, Michael (POL) <Michael.George@pol.state.ma.us>; Perry, Jeffrey (POL) <Jeffrey.Perry@pol.state.ma.us>
Subject: RE: Airlink subscription renewal - TSU

Noah

I don't have visibility into the device subscriptions other than the PO copies (attached and below). Could you work with the BCM rep, Matt, to generate a quote for the renewals needed?

I spoke with Matt yesterday who was looking into this and thought the 91 devices on our July 2022 PO might be unrelated to the coastal camera project.

WORK ORDER NUMBER: #125854 **P.O. NUMBER:** SEE NOTES
PO: 2023BCMCCU12POL20043

Material order request for the following items:

QTY:(91)AIRLINK DEVICE MANAGEMENT (1 YEAR)

WORK ORDER NUMBER: #128361 **P.O. NUMBER:** see notes
PO: 2023BCMCCU12POL20358

Material order request for the following items:

QTY:(60)Sierra Wireless Airlink Basic Subscription (September 1, 2022- August 31, 2023)

Matthew Boschetto
Account Manager | BCM Controls
30 Commerce Way, Woburn, MA 01801
O: 781-897-5178
C: 781-528-8344 | boschettom@bcmcontrols.com

I can assist with processing the renewal PO(s) as necessary – from what you can see in the ALMS account, it may be that a 2 month quote is needed for a partial quantity to cover from now until August 31st, and then we can generate another PO for September 1st , 2023 to August 31st , 2024 for the full amount, if they should all be combined.

Thanks

Gustav Pearson
Accountant IV
Department of State Police
470 Worcester Road

Framingham, MA 01702
508 820-2128 ph
508 820-2165 fax
gustav.pearson@pol.state.ma.us

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Wednesday, June 21, 2023 3:04 PM
To: Pearson, Gustav (POL) <Gustav.Pearson@pol state.ma.us>; George, Michael (POL) <Michael.George@pol.state.ma.us>; Perry, Jeffrey (POL) <Jeffrey.Perry@pol.state.ma.us>
Subject: Re: Airlink subscription renewal - TSU

In our ALMS account, I see 122 Airlink basic devices that are set to expire in September and 17 devices which expired at the end of March.

60 airlink basic devices are covered by the LPR renewal. The 91 for the coastal camera project are not yet included in this system (correct?).

By my math we then need a renewal quote for at least 79 more devices. We also have a number of new devices that are slowly being added, but each of these should have a year included and won't come up for renewal until next year.

What's the status on the renewal of the other devices? Have we received any other renewal quotes? If not, should we have BCM amend the quote for 60 Airlink Basics to reflect a total 140? It would make sense to me to combine all the renewals on one schedule and one quote going forwards, but that decision would ultimately be yours, Lt, if you think that makes sense.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702

From: Pearson, Gustav (POL) <Gustav.Pearson@pol.state.ma.us>
Sent: Wednesday, June 21, 2023 9:34 AM
To: George, Michael (POL) <Michael.George@pol state.ma.us>; Perry, Jeffrey (POL) <Jeffrey.Perry@pol.state.ma.us>
Cc: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Airlink subscription renewal - TSU

Good morning all

I want to ask if BCM has been in touch regarding the renewal for the attached PO (1st attachment). I CC'd Sgt. Pack because I know there was some cross over with 60 additional devices on a separate PO (2nd PO attached for reference – service renewal start date is 9/1/23 for Sgt. Pack's)

WORK ORDER NUMBER: #125854 **P.O. NUMBER:** SEE NOTES
PO: 2023BCMCCU12POL20043

Material order request for the following items:

QTY:(91)AIRLINK DEVICE MANAGEMENT (1 YEAR)

WORK ORDER NUMBER: #128361 **P.O. NUMBER:** see notes
PO: 2023BCMCCU12POL20358

Material order request for the following items:

QTY:(60)Sierra Wireless Airlink Basic Subscription (September 1, 2022- August 31, 2023)

I reached out to Matt at BCM also but want to secure and process an order asap if the 91 devices need to be renewed.

Thank you

Gustav Pearson
Accountant IV
Department of State Police
470 Worcester Road
Framingham, MA 01702
508 820-2128 ph
508 820-2165 fax
gustav.pearson@pol.state.ma.us

From: Mboka-Boyer, Vicky (OGR)
To: Gray, Kellie (POL)
Subject: FW: ALPR Cameras accessories
Date: Monday, June 26, 2023 8:56:39 AM
Attachments: image003.png
image004.png
RE Outstanding items - and requests.msg
image006.png

Hi Kellie,

Here is the ISA I sent you last month. Just sign it and return to me; there is no harm if you complete the project ahead of ISA end date.

Thank you

Vicky Mboka-Boyer
Program Coordinator
Office of Grants and Research, Homeland Security Division
35 Braintree Hill Office Park, Suite 302
Braintree, MA 02184
781-535-0090

Sign up to be notified of grant funding opportunities from OGR.

From: Mboka-Boyer, Vicky (OGR)
Sent: Monday, June 26, 2023 8:51 AM
To: Gray, Kellie (POL) <Kellie.Gray@pol.state.ma.us>
Subject: RE: ALPR Cameras accessories
Importance: High

Hi Kellie,

Can you call me please? We already started an extension request back in May where you requested an extension to 2/29/24. If I already sent you the ISA, could you just sign it and return it to me?

Pleas advise

Vicky Mboka-Boyer
Program Coordinator
Office of Grants and Research, Homeland Security Division
35 Braintree Hill Office Park, Suite 302
Braintree, MA 02184
781-535-0090

Sign up to be notified of grant funding opportunities from OGR.

From: Gray, Kellie (POL) <Kellie.Gray@pol.state.ma.us>
Sent: Wednesday, June 21, 2023 9:37 AM

To: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Cc: Schey, Sonya (OGR) <sonya.schey@mass.gov>; Pryme, Corine A. (OGR) <Corine.A.Pryme@mass.gov>
Subject: RE: ALPR Cameras accessories

Hi Vicky,

I respectfully would like to request an extension till September 30, 2023, on FSHSP20CFC. The items we'd like to purchase attached that you approved on June 12th, could run into delays with delivery.

Thank you,
Kellie

From: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Sent: Monday, June 12, 2023 1:59 PM
To: Gray, Kellie (POL) <Kellie.Gray@pol.state.ma.us>
Subject: ALPR Cameras accessories

Hi Kellie,

Request to purchase accessories for the ALPR Cameras as per attached, is approved.

Thank you

Vicky Mboka-Boyer
Program Coordinator
Office of Grants and Research, Homeland Security Division
35 Braintree Hill Office Park, Suite 302
Braintree, MA 02184
781-535-0090

Sign up to be notified of grant funding opportunities from OGR.

From: Gray, Kellie (POL) <Kellie.Gray@pol.state.ma.us>
Sent: Thursday, June 8, 2023 9:22 AM
To: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Subject: FSHSP20CFC Grant - ends 07/31/2023

Good morning Vicky,

On the FSHSP20CFC Grant, we have about $8000 left due to Prompt pay discounts. We'd like to purchase some accessories to the ALPR Cameras that were purchased. See quotes attached. Please advise and confirm if purchases are approved.

Thank you,
Kellie

Kellie Gray
Deputy Director of Grants & Special Projects
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508 820 -2686
Kellie.gray@pol.state.ma.us

From: Staples, Jennifer (POL)
To: Pack, Noah (POL); Walczak, Ryan (POL)
Cc: Cyr, Mark (POL)
Subject: FW: ALPR Cameras and FLOCK
Date: Thursday, September 21, 2023 9:43:07 AM
Attachments: image001.png

Hi All:

Can we send the updated ALPR policy to John Melander in EOPSS?

Thanks!

Jennifer M. Staples
Chief Legal Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Tel: (508) 820-2307
Cell: [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: Melander, John (EPS) <John.Melander@mass.gov>
Sent: Thursday, September 21, 2023 8:58 AM
To: Walker, Suleyken (EPS) <Suleyken.Walker@mass.gov>; Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>; Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Kwon, Gina K. (EPS) <Gina.K.Kwon@mass.gov>
Subject: Re: ALPR Cameras and FLOCK

Correct. We met last week. They are sending me updated policy (it was updated in June). If it's helpful, I can put together a short internal memo for discussion purposes and/or schedule an internal meeting to debrief.

Thanks,
John

Get Outlook for iOS

From: Walker, Suleyken (EPS) <Suleyken.Walker@mass.gov>
Sent: Thursday, September 21, 2023 8:48:07 AM
To: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>; Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Kwon, Gina K. (EPS) <Gina.K.Kwon@mass.gov>; Melander, John (EPS) <John.Melander@mass.gov>
Subject: RE: ALPR Cameras and FLOCK

Yes. John, this is the meeting you went to right?

Suleyken D. Walker, Esq.
Mobile: [redacted]
Suleyken.Walker@mass.gov

From: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Sent: Thursday, September 21, 2023 8:37 AM
To: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Kwon, Gina K. (EPS) <Gina.K.Kwon@mass.gov>; Walker, Suleyken (EPS) <Suleyken.Walker@mass.gov>; Melander, John (EPS) <John.Melander@mass.gov>
Subject: RE: ALPR Cameras and FLOCK

Did this get set up ?

From: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>
Sent: Wednesday, September 6, 2023 12:46 PM
To: Kwon, Gina K. (EPS) <Gina.K.Kwon@mass.gov>; Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>; Walker, Suleyken (EPS) <Suleyken.Walker@mass.gov>; Melander, John (EPS) <John.Melander@mass.gov>
Subject: ALPR Cameras and FLOCK

Hi All:

Could we schedule a time next week to discuss with Colonel Cyr and the ALPR folks MSP purchasing a FLOCK ALPR Camera subscription? Not FLOCK cameras, but a subscription in order to access data.

Sue, I included you because you were originally involved in ALPR cameras, but feel free to bow out. ☺

Let me know if maybe Tuesday or Wednesday work.

Thanks!!

Jennifer M. Staples

Chief Legal Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Tel: (508) 820-2307
Cell: [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.

Subject: FW: ALPR Policy -
Date: Monday, October 2, 2023 3:09:01 PM
Attachments: TRF-11 Automatic License Plate Recognition (5).pdf
TRF-11 Automatic License Plate Recognition (6).pdf

From:	Warren, Rosemary (POL)
To:	Condlin, Christopher (POL)
Cc:	Serra, Anthony F (POL)
Subject:	FW: ALPR Policy -
Date:	Monday, October 2, 2023 3:10:00 PM
Attachments:	TRF-11 Automatic License Plate Recognition (5).pdf TRF-11 Automatic License Plate Recognition (6).pdf

Good Afternoon Sergeant Condlin,

Can you assist Legal with this information?

Respectfully,

Rose

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

From: Serra, Anthony F (POL) <Anthony.F.Serra@pol.state.ma.us>
Sent: Monday, October 2, 2023 3:05 PM
To: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>
Subject: ALPR Policy -

Hi Rose,

Do you have a copy of the ALPR policy in effect in April of 2020? I was only able to locate the 2 attached policies. Thank you very much.

Anthony Serra
Staff Legal Counsel
Office of Chief Legal Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Telephone: (508) 820-2391

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.

Subject: FW: ALPR Policy & Use
Date: Wednesday, July 5, 2023 12:03:24 PM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

To All:

Effective immediately no Dispatcher is to use any License Plate camera software if you may still have any access. Only the Watch Center and Fusion Center have the authority to perform these functions. Please take the time to read the Department Policy attached. Any questions please see me

---

From: Handfield, Kenneth (POL) <kenneth.handfield@pol.state.ma.us>
To: Snow, Corrine (POL) <corrine.snow@pol.state.ma.us>; Dunbar, Cameron (POL) <Cameron.Dunbar@pol.state.ma.us>; Demers, Joanne (POL) <joanne.demers@pol.state.ma.us>; Ross, Jonathan (POL) <jonathan.ross@pol.state.ma.us>; Keville, Robert (POL) <robert.keville@pol.state.ma.us>; Gleason, Kristin (POL) <kristin.gleason@pol.state.ma.us>; Cheverie, Peter (POL) <peter.cheverie@pol.state.ma.us>; Quinn, Heather (POL) <heather.quinn@pol.state.ma.us>; Teevens, Richard (POL) <richard.teevens@pol.state.ma.us>; Dunphy, Thomas J (POL) <thomas.dunphy@pol.state.ma.us>
Subject: ALPR Policy & Use

Sups,

Please make the attached policy known to your dispatchers. As it reads, the Commonwealth Watch Center and the Commonwealth Fusion Center are the primary ALPR resources for the Department; and any non-Department ALPR Systems accounts are prohibited unless approved by the Division Commander of Homeland Security and Preparedness, through your chain of command.

If your center or any of its personnel have Department ALPR and/or non-Department ALPR accounts, please let me know by end-of-week so a determination can be made about access and use.

Thank you,
Ken

_____

Kenneth E. Handfield, Jr.
Director of Dispatch Services

Massachusetts State Police
Communications Section, Dispatch Services Unit
50 Maple Street, Rm. 2330
Milford, MA 01757

Office: 508.820.2347
Cell & Text: [redacted]

Fax: 774.462.3768 (Milford)

Email: Kenneth.Handfield@Mass.gov

From: Demers, Joanne (POL)
To: Eldridge, Kimberly (POL); Chaves, Daniel (POL); Swiers, Brian (POL); Cataldo, Matthew (POL); McCann, Joseph M. (POL); Ronayne, Adam (POL); McKinnon, Stephanie (POL); Prats, Andrew (POL)
Subject: FW: ALPR Policy & Use
Date: Wednesday, June 28, 2023 1:43:02 PM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

All DHQ Dispatchers:

Please read the attached policy you should have all received in your work email and sign off on it (Front of the dispatch book) when you are next in. It is imperative that we log each entry we make and remove from active log once canceled. D Troop set the standard for this statewide and the policy reflects our diligence. Also be sure that all LPR request through the Fusion center are MSP related or BOLO's for D Troop. I will update the policy and procedure book once you all sign off you have read in its entirety.

Thank you for your time!!

Joanne

Joanne E. Demers (SPD III-ID# C545)
Communications Center Supervisor
SP Middleboro Headquarters
326 West Grove Street
Middleboro, MA 02346
508-947-8087 work
[redacted] cell
508-923-4310 fax
Joanne.Demers@pol.state.ma.us

From: Keville, Robert (POL)
To: Grensavitch, Kenneth (POL); Walker, Kimberly (POL); Shea, Paul (POL); Annunziata, Scott (POL); Girouard, Melissa L (POL); Gutowski, Elizabeth (POL); Cawley, Patrick (POL)
Subject: FW: ALPR Policy & Use
Date: Wednesday, June 28, 2023 8:12:55 AM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

Morning all,

Please see attached Policy as sent by Director Handfield. As stated if you have an ALPR please let me know by the end of the week, so I can forward it the Director Handfield for consideration.

Thank you,

Bob

Robert R. Keville
State Police Dispatcher III
Troop-C Communications
612 Main St,
Holden, Ma. 01529
Phone: 508-829-8420
Fax: 508-829-8421

From: Handfield, Kenneth (POL)
Sent: Tuesday, June 27, 2023 3:05 PM
To: Snow, Corrine (POL); Dunbar, Cameron (POL); Demers, Joanne (POL); Ross, Jonathan (POL); Keville, Robert (POL); Gleason, Kristin (POL); Cheverie, Peter (POL); Quinn, Heather (POL); Teevens, Richard (POL); Dunphy, Thomas J (POL)
Subject: ALPR Policy & Use

Sups,

Please make the attached policy known to your dispatchers. As it reads, the Commonwealth Watch Center and the Commonwealth Fusion Center are the primary ALPR resources for the Department; and any non-Department ALPR Systems accounts are prohibited unless approved by the Division Commander of Homeland Security and Preparedness, through your chain of command.

If your center or any of its personnel have Department ALPR and/or non-Department ALPR accounts, please let me know by end-of-week so a determination can be made about access and use.

Thank you,
Ken

Kenneth E. Handfield, Jr.
Director of Dispatch Services

Massachusetts State Police

Communications Section, Dispatch Services Unit
50 Maple Street, Rm. 2330
Milford, MA 01757

Office: 508.820.2347
Cell & Text: [redacted]

Fax: 774.462.3768 (Milford)

Email: Kenneth.Handfield@Mass.gov

From: Quinn, Heather (POL)
To: Bona, Alexander (POL); Bruso, Matthew (POL); Burgess, Donna (POL); Connell, Jason (POL); Dunbar, Cameron (POL); Emery, Sarah (POL); Harker, Amanda (POL); Jordan, Samantha T. (POL); Kelley, Louise (POL); Patterson, Douglas (POL); Waldron, Ryan (POL); Walker, Colleen (POL); Walsh, Tammy (POL); Wozniak, Alysha (POL)
Subject: FW: ALPR Policy & Use
Date: Tuesday, June 27, 2023 3:30:24 PM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

Hi, everyone,

Attached is the Department's policy regarding ALPR (Automatic License Plate Recognition) resources, please familiarize yourselves with same. From Ken Handfield:

As it reads, the Commonwealth Watch Center and the Commonwealth Fusion Center are the primary ALPR resources for the Department; and any non-Department ALPR Systems accounts are prohibited unless approved by the Division Commander of Homeland Security and Preparedness, through your chain of command.

Please advise if you still have access to the LPR. The last time I tried to use my account (ages ago), it did not work.

Heather

To: B7
Subject: FW: ALPR Policy & Use
Date: Tuesday, June 27, 2023 3:26:00 PM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

Hi, everyone,

Attached is the Department's policy regarding ALPR (Automatic License Plate Recognition) resources. From Ken Handfield:

Please make the attached policy known to your dispatchers. As it reads, the Commonwealth Watch Center and the Commonwealth Fusion Center are the primary ALPR resources for the Department; and any non-Department ALPR Systems accounts are prohibited unless approved by the Division Commander of Homeland Security and Preparedness, through your chain of command.

Please advise if

From: Handfield, Kenneth (POL) <kenneth.handfield@pol.state.ma.us>
Sent: Tuesday, June 27, 2023 3:05 PM
To: Snow, Corrine (POL) <corrine.snow@pol.state.ma.us>; Dunbar, Cameron (POL) <Cameron.Dunbar@pol.state.ma.us>; Demers, Joanne (POL) <joanne.demers@pol.state.ma.us>; Ross, Jonathan (POL) <jonathan.ross@pol.state.ma.us>; Keville, Robert (POL) <robert.keville@pol.state.ma.us>; Gleason, Kristin (POL) <kristin.gleason@pol.state.ma.us>; Cheverie, Peter (POL) <peter.cheverie@pol.state.ma.us>; Quinn, Heather (POL) <heather.quinn@pol.state.ma.us>; Teevens, Richard (POL) <richard.teevens@pol.state.ma.us>; Dunphy, Thomas J (POL) <thomas.dunphy@pol.state.ma.us>
Subject: ALPR Policy & Use

Sups,

Please make the attached policy known to your dispatchers. As it reads, the Commonwealth Watch Center and the Commonwealth Fusion Center are the primary ALPR resources for the Department; and any non-Department ALPR Systems accounts are prohibited unless approved by the Division Commander of Homeland Security and Preparedness, through your chain of command.

If your center or any of its personnel have Department ALPR and/or non-Department ALPR accounts, please let me know by end-of-week so a determination can be made about access and use.

Thank you,
Ken

Kenneth E. Handfield, Jr.
Director of Dispatch Services

Massachusetts State Police
Communications Section, Dispatch Services Unit

50 Maple Street, Rm. 2330
Milford, MA 01757

Office: 508.820.2347
Cell & Text: [redacted]

Fax: 774.462.3768 (Milford)

Email: Kenneth.Handfield@Mass.gov

From: Gleason, Kristin (POL)
To: Fredholm, Shana (POL); Ortins, Lauren (POL); Levesque, Joseph (POL); Doherty, Molly (POL)
Cc: Gleason, Kristin (POL)
Subject: Fw: ALPR Policy & Use
Date: Monday, July 31, 2023 6:55:15 PM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

FYI-

Kristin M Gleason
State Police Dispatcher III, C437
Troop F Communications
2 Service Road
East Boston, MA 02128
(Phone) 617-568-7300
(Fax) 617-568-7520
(Cell) [redacted]

Sups,

Please make the attached policy known to your dispatchers. As it reads, the Commonwealth Watch Center and the Commonwealth Fusion Center are the primary ALPR resources for the Department; and any non-Department ALPR Systems accounts are prohibited unless approved by the Division Commander of Homeland Security and Preparedness, through your chain of command.

If your center or any of its personnel have Department ALPR and/or non-Department ALPR accounts, please let me know by end-of-week so a determination can be made about access and use.

Thank you,
Ken

Kenneth E. Handfield, Jr.
Director of Dispatch Services

Massachusetts State Police
Communications Section, Dispatch Services Unit
50 Maple Street, Rm. 2330

Milford, MA 01757

Office: 508.820.2347
Cell & Text: [redacted]

Fax: 774.462.3768 (Milford)

Email: Kenneth.Handfield@Mass.gov

Subject: FW: ALPR Policy Draft
Date: Wednesday, March 1, 2023 3:09:00 PM
Attachments: TRF-11 Automatic License Plate Recognition DRAFT 16 3-1-23.docx

From: Staples, Jennifer (POL)
To: Brunelli, Daniel (POL)
Subject: FW: ALPR Policy Draft
Date: Wednesday, March 1, 2023 3:09:40 PM
Attachments: TRF-11 Automatic License Plate Recognition DRAFT 16 3-1-23.docx
image001.png

Hey Dan:

Lets chat tomorrow or early next week about what language we could add to address the caselaw.

Thanks!!

Jennifer M. Staples
Chief Legal Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Tel: (508) 820-2307
Cell: G.L. c. 4.sec. 7.cl.26 (n)(security)

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: Wednesday, March 1, 2023 1:46 PM
To: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Brunelli, Daniel (POL) <Daniel.Brunelli@pol.state.ma.us>; Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Subject: ALPR Policy Draft

Attach is the latest draft of the revised ALPR policy 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

Subject: FW: ALPR Policy Revision Draft
Date: Tuesday, May 23, 2023 10:08:27 AM
Attachments: TRF-11 Automatic License Plate Recognition DRAFT 2023 (1).docx

---

From: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Sent: Friday, May 5, 2023 1:52 PM
To: Condlin, Christopher (POL) <Christopher.S.Condlin@pol.state.ma.us>
Cc: Powers, Liam (POL) <Liam.J.Powers@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: ALPR Policy Revision Draft

Good afternoon Chris,
Please find attached the ALPR policy revision draft. I believe it will need some formatting. If possible, can we include it in this quarter's batch awaiting promulgation? Legal has already reviewed and approved. Please do not hesitate to reach out with any questions/concerns.

Thank you,
Mark

Lieutenant Colonel Mark D. Cyr #2728

Massachusetts State Police

Division Commander

Division of Homeland Security and Preparedness

508-988-7301 (office)

[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:	Condlin, Christopher (POL)
To:	Powers, Liam (POL)
Subject:	FW: ALPR Policy Revision Draft
Date:	Tuesday, May 23, 2023 10:08:35 AM
Attachments:	TRF-11 Automatic License Plate Recognition DRAFT 2023 (1).docx

From: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Sent: Friday, May 5, 2023 1:52 PM
To: Condlin, Christopher (POL) <Christopher.S.Condlin@pol.state.ma.us>
Cc: Powers, Liam (POL) <Liam.J.Powers@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: ALPR Policy Revision Draft

Good afternoon Chris,
Please find attached the ALPR policy revision draft. I believe it will need some formatting. If possible, can we include it in this quarter's batch awaiting promulgation? Legal has already reviewed and approved. Please do not hesitate to reach out with any questions/concerns.

Thank you,
Mark

Lieutenant Colonel Mark D. Cyr #2728

Massachusetts State Police

Division Commander

Division of Homeland Security and Preparedness

508-988-7301 (office)

[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)
To: Lorenco, Nicholas (POL)
Subject: Fw: ALPR Policy Update
Date: Friday, July 14, 2023 3:13:43 PM
Attachments: TRF-11 Automatic License Plate Recognition.pdf
Mobile Ops & Hit Confirm.jpg

Nick, please forward to all CVES users with ALPR cruisers. Thank you.

Notification of ALPR Policy Update

Each of you is assigned a cruiser with an ALPR system that is either in service or will hopefully be back in service soon. The Department's ALPR policy (TRF-11) was officially updated as of June 27, 2023. An updated copy is attached to this email.

There are no substantive updates that apply specifically to users of cruiser mounted ALPRs. The sections titled "**Mobile Operations**" and "**Hit/Alert Confirmation"** may be helpful to review, and screenshots are attached.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

From: Pack, Noah (POL)
To: Pack, Noah (POL)
Subject: Fw: ALPR Policy Update
Date: Friday, July 14, 2023 3:09:00 PM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

Notification of ALPR Policy Update

Each of you is assigned a cruiser with an ALPR system that is either in service or will hopefully be back in service soon. The Department's ALPR policy (TRF-11) was officially updated as of June 27, 2023. An updated copy is attached to this email.

There are no substantive updates that apply specifically to users of cruiser mounted ALPRs. The section on "**Hit/Alert Confirmation"** was reworded and may be helpful to review:

Prior to initiation of a stop or enforcement action based upon an ALPR hit or alert, members shall confirm the hit or alert, to include:

- Verify the *plate*: Visually verify that the vehicle plate matches the ALPR system's 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 that generated the hit/alert (e.g., is the vehicle still stolen), through:
    - o Criminal Justice Information System (CJIS);
    - o National Crime Information Center (NCIC);
    - o Department's Records Management System (RMS); or
    - o Another appropriate source of data

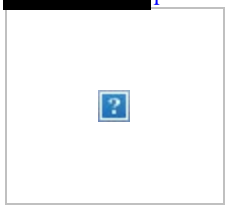
Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

From: Tudryn, Theodore (POL)
To: Alben, Timothy (POL)
Subject: Fw: ALPR Policy Update
Date: Monday, August 28, 2023 11:34:14 AM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

Tpr. T.J. Tudryn #3367
Trooper (T.J.) Theodore J. Tudryn Jr.
Massachusetts State Police
Division of Field Services
B Troop "CAT" Community Action Team (East)
Eve Shift/ Line 2
[redacted] personal mobile



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 message in error, please delete this email immediately.

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Saturday, July 1, 2023 21:07
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: ALPR Policy Update

Notification of ALPR Policy Update

The Department's ALPR policy (TRF-11) was officially updated as of June 27, 2023. An updated copy is attached to this email. This policy governs the use of the ALPR systems by sworn and civilian members of MSP. Please review it to ensure you are familiar with the most recent version. Many of the updates directly reflect the best practices that we have already been using and teaching, such as limiting the scope of searches and the duration of manual hotlist entries.

One noteworthy update is that a manual hotlist entry request must be authorized by a supervisor, except in exigent circumstances/emergencies. This can be satisfied in one of two ways: (1) the request can come directly from a supervisor (Sgt. or above or civilian equivalent),

or (2) the requestor can provide the name of the supervisor who has authorized the request. If you or a member of your unit submits a hotlist request to the Watch Center, they will respond with an inquiry about this authorization if it does not meet one of those criteria in the initial request.

As always please feel free to reach out with questions, comments, or success stories.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

From: Resendes, Eric (POL)
To: Henneberry, Derek (POL)
Subject: Fw: ALPR Update Materials
Date: Monday, October 16, 2023 1:59:24 PM
Attachments: Neology PAGIS-2.15 User training.pdf
TRF-11 Automatic License Plate Recognition.pdf

Respectfully,

Trooper Eric J. Resendes #3698
Massachusetts State Police
Troop D Community Action Team
326 West Grove Street
Middleboro, MA 02346
(508) 961-8887
Eric.Resendes@MassMail.State.MA.US

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Tuesday, August 8, 2023 2:49 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Walczak, Ryan (POL) <ryan.walczak@pol.state.ma.us>
Subject: ALPR Update Materials

Hello all:

Our records indicate that you are currently assigned to a DFS cruiser that has an ALPR system on it. That system is *NOT* currently in service (meaning working and allowed to connect to and receive alerts/hits). We are hopeful that funding will become available to conduct the necessary updates and/or maintenance to your device, and we hope to get your systems online in the reasonably near future.

In preparation, please review the attached training materials. For those who have not previously received it, a familiarization training either in-person or via remote meeting/call will also be provided.

You are required to review these materials prior to having the ALPR systems on your cruisers activated or re-activated:

1. General Order TRF-11, the Department's ALPR policy
2. Neology PAGIS 2.15 User Training, a pdf document

Please reply to this message, including Sergeant Ryan Walczak of the Technical Services Unit, indicating when you have reviewed the materials and if you understand them or have any questions.

Respectfully,

Sergeant Noah H. Pack
Massachusetts State Police

Subject: FW: CT challenges to LPR cameras
Date: Tuesday, February 7, 2023 11:50:40 AM
Attachments: New Haven Register Article Dec 2022.pdf
AUTOMATIC LICENSE PLATE RECOGNITION SYSTEMS.pdf
A&O 13.16.2 LPRs.pdf

Allison Hynes
Staff Legal Counsel
Office of Chief Legal Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Telephone: 508.820.2335

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: Ayers, Kathleen <Kathleen.Ayers@ct.gov>
Sent: Tuesday, February 7, 2023 11:40 AM
To: Brunelli, Daniel (POL) <Daniel.Brunelli@pol.state.ma.us>
Cc: Hynes, Allison E (POL) <Allison.E.Hynes@pol.state.ma.us>
Subject: CT challenges to LPR cameras

CAUTION: This email originated from a sender outside of the 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 Dan

I did some quick looking this morning and I did not find any court challenges to CT police's use of license plate reader cameras. The ACLU has been vocal about their concerns re: privacy and retention, but the one bill proposed in 2012 that would have limited retention to 2 weeks did not pass the House.

Also, I couldn't find the 5-year retention period that my colleague referred to yesterday. Instead, I see that our own State Police A&O Manual policy lists retention at 90 days unless the footage is tagged as evidence. That is the same policy we use for all our camera footage.

I attached to this email some more materials that might be helpful. The newspaper article contains a link to a 2019 ACLU report that is over 1,000 pages; it may provide a glimpse into any potential challenges.

Please let me know what else I could look into to help you all with this.

Thank you,

Kate Ayers
Staff Attorney 2
Department of Emergency Services and Public Protection
Phone: (860)-685-8150
Fax: (860)-685-8611
kathleen.ayers@ct.gov

NOTICE: This e-mail transmission and any accompanying attachments may contain confidential or privileged information. They are intended for use by the individual or entity named on this e-mail transmission. If you are not the intended recipient, you are not authorized to disclose, copy, distribute or use, in any manner, the contents of this information. If you have received this e-mail transmission in error, please notify us by e-mail immediately.

From: Hynes, Allison E (POL)
To: Staples, Jennifer (POL)
Cc: Brunelli, Daniel (POL)
Subject: FW: CT challenges to LPR cameras
Date: Tuesday, February 7, 2023 11:51:07 AM
Attachments: New Haven Register Article Dec 2022.pdf
AUTOMATIC LICENSE PLATE RECOGNITION SYSTEMS.pdf
A&O 13.16.2 LPRs.pdf

Hi Jen- FYI

Allison Hynes
Staff Legal Counsel
Office of Chief Legal Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Telephone: 508.820.2335

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: Ayers, Kathleen <Kathleen.Ayers@ct.gov>
Sent: Tuesday, February 7, 2023 11:40 AM
To: Brunelli, Daniel (POL) <Daniel.Brunelli@pol.state.ma.us>
Cc: Hynes, Allison E (POL) <Allison.E.Hynes@pol.state.ma.us>
Subject: CT challenges to LPR cameras

CAUTION: This email originated from a sender outside of the 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 Dan

I did some quick looking this morning and I did not find any court challenges to CT police's use of license plate reader cameras. The ACLU has been vocal about their concerns re: privacy and retention, but the one bill proposed in 2012 that would have limited retention to 2 weeks did not pass the House.

Also, I couldn't find the 5-year retention period that my colleague referred to yesterday. Instead, I see that our own State Police A&O Manual policy lists retention at 90 days unless the footage is tagged as evidence. That is the same policy we use for all our camera footage.

I attached to this email some more materials that might be helpful. The newspaper article contains a

link to a 2019 ACLU report that is over 1,000 pages; it may provide a glimpse into any potential challenges.

Please let me know what else I could look into to help you all with this.

Thank you,

Kate Ayers
Staff Attorney 2
Department of Emergency Services and Public Protection
Phone: (860)-685-8150
Fax: (860)-685-8611
kathleen.ayers@ct.gov

NOTICE: This e-mail transmission and any accompanying attachments may contain confidential or privileged information. They are intended for use by the individual or entity named on this e-mail transmission. If you are not the intended recipient, you are not authorized to disclose, copy, distribute or use, in any manner, the contents of this information. If you have received this e-mail transmission in error, please notify us by e-mail immediately.

From: Yereniuk, Anne (NWD)
To: "Erick Fredette"
Cc: Lemay, Joshua (POL); Bova, Anthony (POL); Skorupa, Sergei (POL); Odierna, Lori (NWD)
Subject: FW: Email: Commonwealth v. McCarthy_ 484 Mass. 493
Date: Friday, October 27, 2023 1:05:22 PM
Attachments: Commonwealth v. McCarthy_ 484 Mass. 493.pdf

Hi Erick,
Attached is the McCarthy decision regarding Automatic License Plate Readers issued in 2020.

Since I was chatting about it with SPDU, I'm CCing them as well and Lori too.

The decision is interesting and doesn't have a bright line, but gives a warning that my initial gut reaction that we should get a SW is on point.

Eyewitness surveillance for motor vehicle plates in the public does not implicate any reasonable expectation of privacy interest.

However, ALPR (automatic license plate readers) does and is analogous to cell site location information in cell towers. The Court opined that police surveillance using technology (as opposed to eye witness observations of plates in connection to traffic stops) does implicate privacy interests even though the vehicles are operating on public ways.

What the Court has termed as the "mosaic theory" that the Court developed in Augustine (which was the case where the Court held we need a SW for CSLI data) applies here. You don't need a SW for a one-time ping under exigency, because a one-time ping for CSLI doesn't show all the physical movements over a period of time. Similarly, the SJC in the McCarthy case found that the data from the ALPRs to be limited in scope since it was limited to the Bourne and Sagamore Bridges for a limited period of time.

However, under mosaic theory, when collected for a long period of time the "cumulative nature of the information collected implicates a privacy interest on the part of the individual who is the target of the trackings." The length of time that the CSLI is being requested is a factor that the investigator should get a SW. The Court holds in McCarthy that ALPR is analogous so that we would need to probably get a SW if you are requesting data for a longer period of time.

I think that if you were just looking at a distinct date/location for the sex offender's plate that under McCarthy you wouldn't need a SW.

However, now that you have told me that there's some indication that the child was in communication as far back as two years before she went missing when she was only 14 y.o., we need to request the longest possible period of time in which the Commonwealth keeps the ALPR data.

We aren't allowed to get CSLI data via a Grand Jury subpoena. Since the McCarthy court compares ALPR to CSLI data, I think that the Court would similarly rule that we cannot get that location data via a Grand Jury subpoena, so let's get a SW.

Also I think I'd rather go to Superior Court on this since it is a novel not typically every day thing that goes to District Court. Let's meet up next week to draft this SW together. If you could get info for how far back that this data is retained that would be helpful.

Great working with you.

Thanks,
~ Anne

Anne Yereniuk| Assistant District Attorney
Deputy Chief of the Child Abuse Unit
Northwestern District Attorney's Office
anne.yereniuk@mass.gov| NorthwesternDA.org
1 Gleason Plaza | Northampton, MA 01060
Office (413) 586-9225 | **Fax** (413) 584-3635
Please view our Annual Report and connect with the NWDAO on Facebook

---

From: LexisNexisDelivery@lexisnexis.com <LexisNexisDelivery@lexisnexis.com>
Sent: Friday, October 27, 2023 12:39 PM
To: Yereniuk, Anne (NWD) <anne.yereniuk@mass.gov>; Yereniuk, Anne (NWD) <anne.yereniuk@mass.gov>
Subject: Email: Commonwealth v. McCarthy_ 484 Mass. 493

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

Delivery

About LexisNexis | Privacy Policy | Terms & Conditions | Copyright © 2023 LexisNexis.

* This is an automated email. Please do not reply to this email address.

This e-mail message is generated from the Office of the Northwestern 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: Hession, Paul (POL)
To: Brooks, Brian (POL)
Subject: FW: Genetec Citigraf overview
Date: Tuesday, May 16, 2023 11:35:15 AM
Attachments: logocolor(2)_89b44f7c-382f-4530-aee7-d61e3804cc0f.png
emailsignature_ad2b160d-0a28-4983-a2d6-92a7559aa4d9.png
EN-Genetec-Citigraf-Brochure.pdf
Citigraf - Overview.pdf

Lt. Brooks,

FYI

Thanks
Paul

From: Jason Bianco <jason.bianco@signetgroup.net>
Sent: Friday, April 7, 2023 9:14 AM
To: Hession, Paul (POL) <Paul.Hession@pol.state.ma.us>
Subject: Genetec Citigraf overview

CAUTION: This email originated from a sender outside of the 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 Paul,

I'm not sure if you are aware but wanted to share one of Genetec's products called Citigraf. I attached a general brochure as well as on overview.

In brief summary, it provides a real time crime center integrated to your CAD program as well as GIS and ESRI mapping……and of course being the same platform that you use for video surveillance, license plate recognition, access control, emergency communications and alarm monitoring.

I could coordinate a demonstration if there is any interest on your part.

Thank you.

Jason Bianco
VP, Mission Critical Systems

90 Longwater Drive, Norwell, MA 02061
E: jason.bianco@signetgroup.net
M: (781) 883-6624
signetgroup.net

INNOVATION • COLLABORATION • INTEGRITY

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you are not the intended recipient you are notified that disclosing, copying, distributing, or taking any action in reliance on the contents of this

information is strictly prohibited. If you have received this email in error, please notify the sender immediately and delete this email from your system.

Subject: FW: Genetec Citigraf overview
Date: Tuesday, May 16, 2023 11:34:50 AM
Attachments: logocolor(2)_89b44f7c-382f-4530-aee7-d61e3804cc0f.png
emailsignature_ad2b160d-0a28-4983-a2d6-92a7559aa4d9.png
EN-Genetec-Citigraf-Brochure.pdf
Citigraf - Overview.pdf

From: Jason Bianco <jason.bianco@signetgroup.net>
Sent: Friday, April 7, 2023 9:14 AM
To: Hession, Paul (POL) <Paul.Hession@pol.state.ma.us>
Subject: Genetec Citigraf overview

CAUTION: This email originated from a sender outside of the 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 Paul,

I'm not sure if you are aware but wanted to share one of Genetec's products called Citigraf. I attached a general brochure as well as on overview.

In brief summary, it provides a real time crime center integrated to your CAD program as well as GIS and ESRI mapping……and of course being the same platform that you use for video surveillance, license plate recognition, access control, emergency communications and alarm monitoring.

I could coordinate a demonstration if there is any interest on your part.

Thank you.

Jason Bianco
VP, Mission Critical Systems

90 Longwater Drive, Norwell, MA 02061
E: jason.bianco@signetgroup.net
M: (781) 883-6624
signetgroup.net



This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you are not the intended recipient you are notified that disclosing, copying, distributing, or taking any action in reliance on the contents of this information is strictly prohibited. If you have received this email in error, please notify the sender immediately and delete this email from your system.

From: Brooks, Brian (POL)
To: Bender, Sean (POL)
Subject: FW: Genetec Citigraf overview
Date: Friday, May 19, 2023 8:52:00 AM
Attachments: logocolor(2)_89b44f7c-382f-4530-aee7-d61e3804cc0f.png
emailsignature_ad2b160d-0a28-4983-a2d6-92a7559aa4d9.png
EN-Genetec-Citigraf-Brochure.pdf
Citigraf - Overview.pdf

Thoughts?

From: Hession, Paul (POL) <Paul.Hession@pol.state.ma.us>
Sent: Tuesday, May 16, 2023 11:35 AM
To: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Subject: FW: Genetec Citigraf overview

Lt. Brooks,

FYI

Thanks
Paul

From: Jason Bianco <jason.bianco@signetgroup.net>
Sent: Friday, April 7, 2023 9:14 AM
To: Hession, Paul (POL) <Paul.Hession@pol.state.ma.us>
Subject: Genetec Citigraf overview

CAUTION: This email originated from a sender outside of the 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 Paul,

I'm not sure if you are aware but wanted to share one of Genetec's products called Citigraf. I attached a general brochure as well as on overview.

In brief summary, it provides a real time crime center integrated to your CAD program as well as GIS and ESRI mapping……and of course being the same platform that you use for video surveillance, license plate recognition, access control, emergency communications and alarm monitoring.

I could coordinate a demonstration if there is any interest on your part.

Thank you.

Jason Bianco
VP, Mission Critical Systems

90 Longwater Drive, Norwell, MA 02061
E: jason.bianco@signetgroup.net
M: (781) 883-6624
signetgroup.net



This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you are not the intended recipient you are notified that disclosing, copying, distributing, or taking any action in reliance on the contents of this information is strictly prohibited. If you have received this email in error, please notify the sender immediately and delete this email from your system.

Subject: FW: Genetec Server Spec Sheet
Date: Monday, September 18, 2023 11:05:56 AM
Attachments: EN - Streamvault SV-300E Datasheet (1).pdf

From: Gillham, Nicholas <gillhamn@bcmcontrols.com>
Sent: Monday, September 18, 2023 10:40 AM
To: Hession, Paul (POL) <Paul.Hession@pol.state.ma.us>
Cc: Gillham, Nicholas <gillhamn@bcmcontrols.com>
Subject: Genetec Server Spec Sheet

CAUTION: This email originated from a sender outside of the 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 – for the Foxboro barracks you got the following PN/Model: SV-300E-16T-I5 (SV-300E model, 16 TB of Storage, i5 Intel Processor).
I've attached the datasheet for that specific model.

Let me know if you have any questions
Thanks
Nick

Nick Gillham
Senior Security Applications Engineer
BCM Controls Corporation
Main: 781-933-8878
Direct: 781-897-5111
gillhamn@bcmcontrols.com

From: Pack, Noah (POL)
Subject: Fw: Latest Policy Draft
Date: Monday, March 13, 2023 10:11:19 AM
Attachments: TRF-11 Automatic License Plate Recognition DRAFT 18 3-13-23.docx

---

From: Pack, Noah (POL)
Sent: Monday, March 13, 2023 9:35 AM
To: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Subject: Latest Policy Draft

LTC: latest draft attached.

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: Hernandez, Stephen S. (POL)
To: Ponte, Nicholas R; Rooney, Dave
Subject: Fw: LPR Info
Date: Tuesday, November 7, 2023 1:37:03 PM
Attachments: TRF-11 Automatic License Plate Recognition (3).pdf
image.png
image.png

Trooper Stephen S. Hernandez #3815
Massachusetts State Police
Division of Homeland Security & Preparedness
Narcotics Section - Task Force 1
John F. Kennedy Building - Boston

From: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Sent: Tuesday, November 7, 2023 12:18 PM
To: Hernandez, Stephen S. (POL) <Stephen.S.Hernandez@pol.state.ma.us>
Subject: Re: LPR Info

Good Afternoon,

I have attached a copy of the Department's ALPR policy, TRF-11, which outlines the requirements for requesting a historical query and/or hotlist. Below are the relevant sections.

Historical:

Search Procedures

The Commonwealth Watch Center (CWC) and Commonwealth Fusion Center (CFC) shall serve as the primary ALPR resource for the Department. Search requests submitted to the CWC/CFC shall include, at a minimum:

- Case number or reference;
- Type of investigation or reason for request;
- Plate number(s) and vehicle description (if available);
- Requested search time period; and
- Requested search area (devices or region).

Hotlist:

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, missing person, or kidnapping broadcasts or bulletins;
- Incapacitated or endangered persons;
- Be-On-Look-Out (BOLO) broadcasts or other public safety alerts;
- Investigation of terrorist or criminal offenses; or
- Wanted persons, arrest warrants, or search warrants.

Manual entries onto a Hot List shall be:

- Entered with the vehicle description, if available;
- Entered with a case number or reference;
- Updated or removed when information changes, is no longer current, or is no longer necessary or reasonable;
- Given special attention to rental and short-term use vehicles;
- Given special attention to incidents that may be quickly resolved;
- Entered with an automatic expiration date no longer than thirty (30) days; and
- Approved by a supervisor, except in exigent circumstances.

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: Hernandez, Stephen S. (POL) <Stephen.S.Hernandez@pol.state.ma.us>
Sent: Tuesday, November 7, 2023 11:51 AM
To: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Subject: LPR Info

Good afternoon,

What do we need for LPRs now? Report number and Supervisors authorization?

Trooper Stephen S. Hernandez #3815
Massachusetts State Police
Division of Homeland Security & Preparedness

Narcotics Section - Task Force 1
John F. Kennedy Building - Boston

To: Ronayne, Adam (POL); McCann, Joseph M. (POL)
Subject: FW: LPR Request
Date: Monday, October 23, 2023 7:36:47 AM
Attachments: image001.png
TRF-11 Automatic License Plate Recognition.docx

Read bottom up and be sure your peeps know how this works…

I guess if they ask for a report or incident number we can tell them we will get RAMS number as soon as it is generated to you… If they delay the hit – not on us.

From: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Sent: Monday, October 23, 2023 7:07 AM
To: Demers, Joanne (POL) <joanne.demers@pol.state.ma.us>
Cc: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>; Walczak, Ryan (POL) <ryan.walczak@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Re: LPR Request

Good Morning, Joanne -

Firstly, I apologize for any inconvenience that may have been imposed by the below referenced exchange, however, I hope I can provide some clarity on the situation as it is something that we frequently experience and often results in some confusion / misunderstanding.

I will defer to Det. Lieutenant Brooks, Sergeant Ryan Walczak, and Sergeant Noah Pack to review the Watch Center's handling of the below referenced general BOLO, but I can assure that the intent of our personnel is not to cause a "*huge delay in service"*.

I would encourage all department members seeking to employ ALPR technology in their investigations to familiarize themselves with TRF-11, the Department's Automatic License Plate Recognition technology policy (attached). I have highlighted the relevant portions, which all Watch Center personnel have been instructed to follow during our related training.

Additionally, for your awareness, the Watch Center does also exercise discretion in reviewing both radio and teletype BOLOs for instances in which the exigency of the situation may preclude or supersede the provision of a related case or incident number, and in many instances, we ***will*** query and/or enter short-term hotlists for plates pro-actively with authorization of the duty Lieutenant assigned to the Watch Center. Examples of situations where the employment of ALPR technology for exigent circumstances include: Missing Persons/Silver Alerts/Homicides or other serious violent crimes/Kidnappings/Terroristic or other threats to life.

In this particular instance, I can also confirm that the registration in question ***was*** entered onto the MSP - Troop D - Dispatch hotlist, and remains in the system with a short term expiration date of 10/24/2023 (Ref: Bourne PD - Dom A/B). The

vehicle has not been observed by MSP ALPR since the date/time listed on the original submission.

I hope this helps clarify the reasons for the follow-up question(s) that may be posed by Watch Center personnel when a request for ALPR data and/or hotlist(s) is received. Please do encourage your Dispatchers to continue to submit requests for ALPR data and/or hotlist(s) when appropriate, just also please understand that we may be required (by departmental policy) to pose follow-up questions to ensure the continued and successful access to such a useful investigative tool.

Respectfully,

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

From: Demers, Joanne (POL) <joanne.demers@pol.state.ma.us>
Sent: Sunday, October 22, 2023 6:46 AM
To: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Subject: FW: LPR Request

? email from bottom up –

Hi, my dispatchers are not sure why this new rule is in place…. But a huge delay in service is happening if a report or incident number is needed before anyone can check LPR's???

I was originally told an email was enough to get these started. Has that changed?? I am worried as dispatchers don't get access to RAMS or report numbers and sometimes even the troopers don't have it at the start of an incident, they won't be sure to include the Fusion Center in these requests… I want them to work smarter not harder… The LPR hit in a timely fashion is what often gets things solved or resolved. We can follow up with numbers after the fact, but it is near impossible to expect a number before a request can be made…

Thanks for any help or feedback on this critical item!

Respectfully,

Joanne

Joanne E. Demers (SPD III-ID# C545)
Communications Center Supervisor
SP Middleboro Headquarters
326 West Grove Street
Middleboro, MA 02346
508-947-8087 work
G.L. c. 4.sec. 7.cl.26 (n)(security) cell
508-923-4310 fax
Joanne.Demers@pol.state.ma.us

From: Ronayne, Adam (POL) <Adam.Ronayne@pol.state.ma.us>
Sent: Sunday, October 22, 2023 4:28 AM
To: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Cc: POL-DL-DHQ Communications <POL-DL-DHQCommunications@MassMail.State.MA.US>
Subject: Re: LPR Request

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

Adam Ronayne
State Police Dispatcher II
State Police Middleboro
326 West Grove St.
Middleboro, MA 02346
Work: (508) 947-8087

From: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>

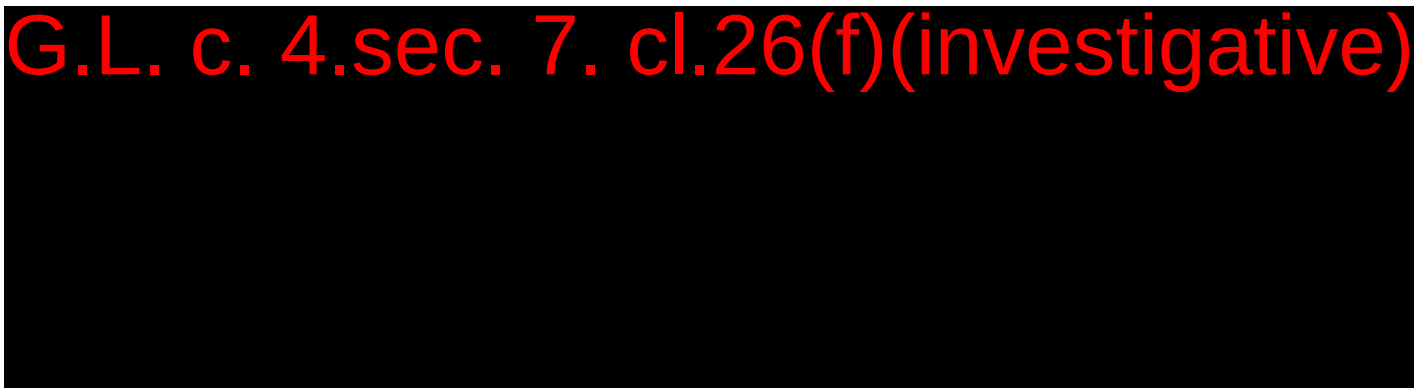
Sent: Sunday, October 22, 2023 4:26 AM
To: Ronayne, Adam (POL) <Adam.Ronayne@pol.state.ma.us>
Subject: RE: LPR Request

Adam,
We need a report/case number to enter it into the hotlist.

Lieutenant Robert P. Quigley Jr. #2777
Massachusetts State Police
Commonwealth Fusion Center
470 Worcester Road
Framingham, MA 01702
508-820-2233

The preceding email message (including any attachments) contains information that may be confidential, may be protected by 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: Ronayne, Adam (POL) <Adam.Ronayne@pol.state.ma.us>
Sent: Sunday, October 22, 2023 4:24 AM
To: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Cc: POL-DL-DHQ Communications <POL-DL-DHQCommunications@MassMail.State.MA.US>
Subject: LPR Request



Adam Ronayne
State Police Dispatcher II
State Police Middleboro
326 West Grove St.
Middleboro, MA 02346

Work: (508) 947-8087



From: Demers, Joanne (POL)
To: Ronayne, Adam (POL); McCann, Joseph M. (POL)
Cc: Chaves, Daniel (POL)
Subject: FW: LPR Request
Date: Monday, October 23, 2023 7:40:06 AM
Attachments: image001.png
TRF-11 Automatic License Plate Recognition.docx

Read from bottom up and be sure your peeps know how this works…

I guess if they ask for a report or incident number, we can tell them we will get RAMS number as soon as it is generated to you… If they delay the hit – not on us. We can only do what we can do with regards to the LPR.

You guys do great and as long as everyone understands that it is not the Fusion center personnel it is POLICY!

Have a great day!!

Joanne

Joanne E. Demers (SPD III-ID# C545)
Communications Center Supervisor
SP Middleboro Headquarters
326 West Grove Street
Middleboro, MA 02346
508-947-8087 work
[redacted] cell
508-923-4310 fax
Joanne.Demers@pol.state.ma.us

From: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Sent: Monday, October 23, 2023 7:07 AM
To: Demers, Joanne (POL) <joanne.demers@pol.state.ma.us>
Cc: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>; Walczak, Ryan (POL) <ryan.walczak@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Re: LPR Request

Good Morning, Joanne -

Firstly, I apologize for any inconvenience that may have been imposed by the below

referenced exchange, however, I hope I can provide some clarity on the situation as it is something that we frequently experience and often results in some confusion / misunderstanding.

I will defer to Det. Lieutenant Brooks, Sergeant Ryan Walczak, and Sergeant Noah Pack to review the Watch Center's handling of the below referenced general BOLO, but I can assure that the intent of our personnel is not to cause a "*huge delay in service"*.

I would encourage all department members seeking to employ ALPR technology in their investigations to familiarize themselves with TRF-11, the Department's Automatic License Plate Recognition technology policy (attached). I have highlighted the relevant portions, which all Watch Center personnel have been instructed to follow during our related training.

Additionally, for your awareness, the Watch Center does also exercise discretion in reviewing both radio and teletype BOLOs for instances in which the exigency of the situation may preclude or supersede the provision of a related case or incident number, and in many instances, we ***will*** query and/or enter short-term hotlists for plates pro-actively with authorization of the duty Lieutenant assigned to the Watch Center. Examples of situations where the employment of ALPR technology for exigent circumstances include: Missing Persons/Silver Alerts/Homicides or other serious violent crimes/Kidnappings/Terroristic or other threats to life.

In this particular instance, I can also confirm that the registration in question ***was*** entered onto the MSP - Troop D - Dispatch hotlist, and remains in the system with a short term expiration date of 10/24/2023 (Ref: Bourne PD - Dom A/B). The vehicle has not been observed by MSP ALPR since the date/time listed on the original submission.

I hope this helps clarify the reasons for the follow-up question(s) that may be posed by Watch Center personnel when a request for ALPR data and/or hotlist(s) is received. Please do encourage your Dispatchers to continue to submit requests for ALPR data and/or hotlist(s) when appropriate, just also please understand that we may be required (by departmental policy) to pose follow-up questions to ensure the continued and successful access to such a useful investigative tool.

Respectfully,

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

From: Demers, Joanne (POL) <joanne.demers@pol.state.ma.us>

Sent: Sunday, October 22, 2023 6:46 AM
To: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Subject: FW: LPR Request

? email from bottom up –

Hi, my dispatchers are not sure why this new rule is in place…. But a huge delay in service is happening if a report or incident number is needed before anyone can check LPR's???

I was originally told an email was enough to get these started. Has that changed?? I am worried as dispatchers don't get access to RAMS or report numbers and sometimes even the troopers don't have it at the start of an incident, they won't be sure to include the Fusion Center in these requests… I want them to work smarter not harder… The LPR hit in a timely fashion is what often gets things solved or resolved. We can follow up with numbers after the fact, but it is near impossible to expect a number before a request can be made…

Thanks for any help or feedback on this critical item!

Respectfully,

Joanne

Joanne E. Demers (SPD III-ID# C545)
Communications Center Supervisor
SP Middleboro Headquarters
326 West Grove Street
Middleboro, MA 02346
508-947-8087 work
[redacted] cell
508-923-4310 fax
Joanne.Demers@pol.state.ma.us

From: Ronayne, Adam (POL) <Adam.Ronayne@pol.state.ma.us>
Sent: Sunday, October 22, 2023 4:28 AM
To: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Cc: POL-DL-DHQ Communications <POL-DL-DHQCommunications@MassMail.State.MA.US>

Subject: Re: LPR Request

[redacted]

Adam Ronayne
State Police Dispatcher II
State Police Middleboro
326 West Grove St.
Middleboro, MA 02346
Work: (508) 947-8087

From: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Sent: Sunday, October 22, 2023 4:26 AM
To: Ronayne, Adam (POL) <Adam.Ronayne@pol.state.ma.us>
Subject: RE: LPR Request

Adam,
We need a report/case number to enter it into the hotlist.

Lieutenant Robert P. Quigley Jr. #2777
Massachusetts State Police
Commonwealth Fusion Center
470 Worcester Road
Framingham, MA 01702
508-820-2233

The preceding email message (including any attachments) contains information that may be confidential, may be protected by 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: Ronayne, Adam (POL) <Adam.Ronayne@pol.state.ma.us>
Sent: Sunday, October 22, 2023 4:24 AM
To: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Cc: POL-DL-DHQ Communications <POL-DL-DHQCommunications@MassMail.State.MA.US>
Subject: LPR Request

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

[redacted]

Adam Ronayne
State Police Dispatcher II
State Police Middleboro
326 West Grove St.
Middleboro, MA 02346
Work: (508) 947-8087

From: Miller, Dianne (POL)
To: Rossi, Gina (POL)
Subject: FW: massDOT question
Date: Wednesday, October 11, 2023 12:05:35 PM
Attachments: image001.png
SCF_MSP_BainCor_executed.pdf
massDOT_telecom_RFR.pdf
Award - Bain Cor AW.pdf

Baincor is used to purchase solar trailers.

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: Silva, Kyra (POL)
To: Biagi, Pamela (POL)
Subject: FW: MassPort/MSP-Cruisers 24 M500 and WiFi Base
Date: Wednesday, September 20, 2023 9:49:00 AM
Attachments: QUOTE-2137661-6MassPortMSP-Cruisers24M500andWiFiBase (6).pdf
2024MOTRLU07POL20232.pdf
MSIAR_INV_1011906651__inv# 8281711482.pdf

Hi,

Can we discuss this?

From: Pearson, Gustav (POL) <Gustav.Pearson@pol.state.ma.us>
Sent: Tuesday, September 19, 2023 4:31 PM
To: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Cc: Liquori, MaryEllen (POL) <MaryEllen.Liquori@pol.state.ma.us>; Rucho, Julie (POL) <Julie.Rucho@pol.state.ma.us>; Doherty, Nancy (POL) <Nancy.Doherty@pol.state.ma.us>
Subject: FW: MassPort/MSP-Cruisers 24 M500 and WiFi Base

Hi Kyra

PC 2024MOTRLU07POL20232 is now in Pend (I was not originally CC'd on this PO which is unusual – see reference PO copy attached)

So far we have one invoice against it (3rd attachment) and MaryEllen is working on the approval/pack slips with MHQ.

Thanks

Gustav Pearson
Accountant IV
Department of State Police
470 Worcester Road
Framingham, MA 01702
508 820-2128 ph
508 820-2165 fax
gustav.pearson@pol.state.ma.us

From: Pearson, Gustav (POL) <Gustav.Pearson@pol.state.ma.us>
Sent: Friday, August 04, 2023 9:48 AM
To: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Cc: Liquori, MaryEllen (POL) <MaryEllen.Liquori@pol.state.ma.us>; Rucho, Julie (POL) <Julie.Rucho@pol.state.ma.us>; Doherty, Nancy (POL) <Nancy.Doherty@pol.state.ma.us>
Subject: RE: MassPort/MSP-Cruisers 24 M500 and WiFi Base

Hi Kyra

Please reference OPAS request# **OTIS24 – 0232**, shipping to Brian Smith at MHQ, per MaryEllen.

Thank you

Gustav Pearson
Accountant IV
Department of State Police
470 Worcester Road
Framingham, MA 01702
508 820-2128 ph
508 820-2165 fax
gustav.pearson@pol.state.ma.us

From: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Sent: Thursday, August 3, 2023 1:56 PM
To: Pearson, Gustav (POL) <Gustav.Pearson@pol.state.ma.us>; Rucho, Julie (POL) <Julie.Rucho@pol.state.ma.us>
Cc: Liquori, MaryEllen (POL) <MaryEllen.Liquori@pol.state.ma.us>
Subject: MassPort/MSP-Cruisers 24 M500 and WiFi Base

Gustav,

Please enter the attached into OPAS for FY24 and encumber under unit 1975, 8100-0102, activity code **FTRP** to the Detail Accounting tab on the encumbrance.

Julie,

This will be charged back to Massport.

Thank you

From: Pearson, Gustav (POL)
To: Silva, Kyra (POL)
Cc: Liquori, MaryEllen (POL); Rucho, Julie (POL); Doherty, Nancy (POL)
Subject: FW: MassPort/MSP-Cruisers 24 M500 and WiFi Base
Date: Tuesday, September 19, 2023 4:30:49 PM
Attachments: QUOTE-2137661-6MassPortMSP-Cruisers24M500andWiFiBase (6).pdf
2024MOTRLU07POL20232.pdf
MSIAR_INV_1011906651__inv# 8281711482.pdf

Hi Kyra

PC 2024MOTRLU07POL20232 is now in Pend (I was not originally CC'd on this PO which is unusual – see reference PO copy attached)

So far we have one invoice against it (3rd attachment) and MaryEllen is working on the approval/pack slips with MHQ.

Thanks

Gustav Pearson
Accountant IV
Department of State Police
470 Worcester Road
Framingham, MA 01702
508 820-2128 ph
508 820-2165 fax
gustav.pearson@pol.state.ma.us

From: Pearson, Gustav (POL) <Gustav.Pearson@pol.state.ma.us>
Sent: Friday, August 04, 2023 9:48 AM
To: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Cc: Liquori, MaryEllen (POL) <MaryEllen.Liquori@pol.state.ma.us>; Rucho, Julie (POL) <Julie.Rucho@pol.state.ma.us>; Doherty, Nancy (POL) <Nancy.Doherty@pol.state.ma.us>
Subject: RE: MassPort/MSP-Cruisers 24 M500 and WiFi Base

Hi Kyra

Please reference OPAS request# **OTIS24 – 0232**, shipping to Brian Smith at MHQ, per MaryEllen.

Thank you

Gustav Pearson
Accountant IV
Department of State Police
470 Worcester Road
Framingham, MA 01702
508 820-2128 ph
508 820-2165 fax
gustav.pearson@pol.state.ma.us

From: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Sent: Thursday, August 3, 2023 1:56 PM
To: Pearson, Gustav (POL) <Gustav.Pearson@pol.state.ma.us>; Rucho, Julie (POL) <Julie.Rucho@pol.state.ma.us>
Cc: Liquori, MaryEllen (POL) <MaryEllen.Liquori@pol.state.ma.us>
Subject: MassPort/MSP-Cruisers 24 M500 and WiFi Base

Gustav,

Please enter the attached into OPAS for FY24 and encumber under unit 1975, 8100-0102, activity code **FTRP** to the Detail Accounting tab on the encumbrance.

Julie,

This will be charged back to Massport.

Thank you

Subject: FW: MassPort/MSP-Cruisers 24 M500 and WiFi Base
Date: Wednesday, September 20, 2023 9:49:40 AM
Attachments: QUOTE-2137661-6MassPortMSP-Cruisers24M500andWiFiBase (6).pdf
2024MOTRLU07POL20232.pdf
MSIAR_INV_1011906651__inv# 8281711482.pdf

From: Pearson, Gustav (POL) <Gustav.Pearson@pol.state.ma.us>
Sent: Tuesday, September 19, 2023 4:31 PM
To: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Cc: Liquori, MaryEllen (POL) <MaryEllen.Liquori@pol.state.ma.us>; Rucho, Julie (POL) <Julie.Rucho@pol.state.ma.us>; Doherty, Nancy (POL) <Nancy.Doherty@pol.state.ma.us>
Subject: FW: MassPort/MSP-Cruisers 24 M500 and WiFi Base

Hi Kyra

PC 2024MOTRLU07POL20232 is now in Pend (I was not originally CC'd on this PO which is unusual – see reference PO copy attached)

So far we have one invoice against it (3rd attachment) and MaryEllen is working on the approval/pack slips with MHQ.

Thanks

Gustav Pearson
Accountant IV
Department of State Police
470 Worcester Road
Framingham, MA 01702
508 820-2128 ph
508 820-2165 fax
gustav.pearson@pol.state.ma.us

From: Pearson, Gustav (POL) <Gustav.Pearson@pol.state.ma.us>

Sent: Friday, August 04, 2023 9:48 AM
To: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Cc: Liquori, MaryEllen (POL) <MaryEllen.Liquori@pol.state.ma.us>; Rucho, Julie (POL) <Julie.Rucho@pol.state.ma.us>; Doherty, Nancy (POL) <Nancy.Doherty@pol.state.ma.us>
Subject: RE: MassPort/MSP-Cruisers 24 M500 and WiFi Base

Hi Kyra

Please reference OPAS request# **OTIS24 – 0232**, shipping to Brian Smith at MHQ, per MaryEllen.

Thank you

Gustav Pearson
Accountant IV
Department of State Police
470 Worcester Road
Framingham, MA 01702
508 820-2128 ph
508 820-2165 fax
gustav.pearson@pol.state.ma.us

From: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Sent: Thursday, August 3, 2023 1:56 PM
To: Pearson, Gustav (POL) <Gustav.Pearson@pol.state.ma.us>; Rucho, Julie (POL) <Julie.Rucho@pol.state.ma.us>
Cc: Liquori, MaryEllen (POL) <MaryEllen.Liquori@pol.state.ma.us>
Subject: MassPort/MSP-Cruisers 24 M500 and WiFi Base

Gustav,

Please enter the attached into OPAS for FY24 and encumber under unit 1975, 8100-0102, activity code **FTRP** to the Detail Accounting tab on the encumbrance.

Julie,

This will be charged back to Massport.

Thank you

To: Driscoll, Elaine (EPS)
Subject: FW: MSP ALPR Procedures
Date: Friday, October 20, 2023 11:49:31 AM
Attachments: image001.png
image003.png

Questions from MassLive below. Highlight is mine. The policy makes clear that we would not enter a plate for another state police department trying to track someone

Dave Procopio
Director, Media Relations Unit
Massachusetts State Police

From: Will Katcher <WKatcher@masslive.com>
Sent: Friday, October 20, 2023 11:34 AM
To: Procopio, David (POL) <david.procopio@pol.state.ma.us>
Subject: Re: MSP ALPR Procedures

Hi Dave,

I very much appreciate it. I've listed a few questions below, but please feel free to include any other comments as well.

We expect to have a story out this weekend. Would you be able to get back to me today?

- Has the hot list been a useful public safety tool, and how so?
- In what cases has the hot list been most helpful? Are there examples or anecdotes of where the hot list had been helpful in locating a person during an emergency?
- What goes into deciding whether to use the hot list? How do troopers determine whether to add a vehicle to the list? Are there cases where it doesn't make sense to use the hot list to find a missing or wanted person? Is the decision to add a vehicle to the hot list up to the State Police, or can local police departments request for vehicles to be added?
- Data privacy advocates have raised concerns about the sharing of location data with out-of-state police departments, out of fear that it could unwittingly expose a person who traveled to Massachusetts for something like reproductive health care. Has that concern been brought to the State Police? How would State Police verify the information it receives from out-of-state departments to ensure it is protecting the privacy of people who travel into this state?

If I can clarify any questions, don't hesitate to let me know.

All my best,
Will

Will Katcher
Reporter
MassLive

339-229-1497

From: Procopio, David (POL) <david.procopio@pol.state.ma.us>
Date: Friday, October 20, 2023 at 9:45 AM
To: Will Katcher <WKatcher@masslive.com>
Subject: MSP ALPR Procedures

Will,

I am going to provide you with our Departmental policy governing the use of our ALPRs. Did you have specific questions you also wanted to pose to us about the process?

Dave Procopio
Director, Media Relations Unit
Massachusetts State Police

From: Procopio, David (POL)
To: Driscoll, Elaine (EPS)
Subject: FW: MSP ALPR Procedures
Date: Friday, October 20, 2023 11:51:00 AM
Attachments: image001.png
image003.png

Questions from MassLive below. Highlight is mine. The policy makes clear that we would not enter a plate for another state police department trying to track someone coming to this state for an activity that is legal here.

Dave Procopio
Director, Media Relations Unit
Massachusetts State Police

From: Will Katcher <WKatcher@masslive.com>
Sent: Friday, October 20, 2023 11:34 AM
To: Procopio, David (POL) <david.procopio@pol.state.ma.us>
Subject: Re: MSP ALPR Procedures

Hi Dave,

I very much appreciate it. I've listed a few questions below, but please feel free to include any other comments as well.

We expect to have a story out this weekend. Would you be able to get back to me today?

- Has the hot list been a useful public safety tool, and how so?
- In what cases has the hot list been most helpful? Are there examples or anecdotes of where the hot list had been helpful in locating a person during an emergency?
- What goes into deciding whether to use the hot list? How do troopers determine whether to add a vehicle to the list? Are there cases where it doesn't make sense to use the hot list to find a missing or wanted person? Is the decision to add a vehicle to the hot list up to the State Police, or can local police departments request for vehicles to be added?
- Data privacy advocates have raised concerns about the sharing of location data with out-of-state police departments, out of fear that it could unwittingly expose a person who traveled to Massachusetts for something like reproductive health care. Has that concern been brought to the State Police? How would State Police verify the information it receives from out-of-state departments to ensure it is protecting the privacy of people who travel into this state?

If I can clarify any questions, don't hesitate to let me know.

All my best,
Will

Will Katcher

Reporter
MassLive
339-229-1497

From: Procopio, David (POL) <david.procopio@pol.state.ma.us>
Date: Friday, October 20, 2023 at 9:45 AM
To: Will Katcher <WKatcher@masslive.com>
Subject: MSP ALPR Procedures

Will,

I am going to provide you with our Departmental policy governing the use of our ALPRs. Did you have specific questions you also wanted to pose to us about the process?

Dave Procopio
Director, Media Relations Unit
Massachusetts State Police

From: Kwon, Gina K. (EPS)
To: Cyr, Mark (POL)
Subject: FW: MSP and DOT Equipment Collocation Request
Date: Monday, August 14, 2023 3:02:06 PM
Attachments: MSP DHS DOT Collocation Request 10-2022 Letterheard (8).doc
MSP DHS DOT Collocation Request 7-23 Notes Update.doc

I'm meeting with DOT on Wednesday at 2. Can I grab you for like 5-10 at some point tomorrow to make sure I have this all correctly and just get an update (if any) on any changes since you sent this up…I know it's been a bit.

Gina K. Kwon
Undersecretary for Law Enforcement
Mobile: [redacted]

From: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Sent: Wednesday, July 5, 2023 2:39 PM
To: Kwon, Gina K. (EPS) <Gina.K.Kwon@mass.gov>; Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Cc: Mawn, John (POL) <John.Mawn@pol.state.ma.us>; Pinkham, John (POL) <john.pinkham@pol.state.ma.us>; Wheeler, Mark (POL) <Mark.Wheeler@pol.state.ma.us>; Diotte, Jeffrey (POL) <jeffrey.diotte@pol.state.ma.us>
Subject: MSP and DOT Equipment Collocation Request

Good afternoon U/S Kwon and Terrey,
I have attached a letter that I sent to Joe Foti and Tony Wade (MA DOT) on October 26, 2022, requesting collocation of equipment, specifically ALPR cameras. In this letter, I highlighted the criticality of this equipment as it pertains to our public safety mission and detailed the nature of the request, the responsibilities the MSP would assume, and the anticipated sites for deployment of the cameras.

As discussed yesterday, Mr. Wade recently informed Sgt. Pack the DOT has not historically allowed MSP access to State resources, and this request would require a "policy change."

For a better understanding and to assist with the next steps, I have attached a Word document outlining a history of the request to include why this request benefits the Commonwealth. Unfortunately, in order to enable a "policy change," the next step in this request may have to be facilitated through respective Secretariats.

Please let me know if you have any questions/concerns.

Thank you!
Mark

Lieutenant Colonel Mark D. Cyr #2728

Massachusetts State Police

Division Commander

Division of Homeland Security and Preparedness

508-988-7301 (office)

G.L. c. 4.sec. 7.cl.26 (n)(security) *(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: Banik, John (POL)
To: Condlin, Christopher (POL)
Subject: Fw: Pilot- Final Data summary
Date: Monday, March 6, 2023 11:14:14 AM
Attachments: MSP-Final Data.pdf

From: LENEHAN, DENIS R <dl009w@att.com>
Sent: Friday, March 3, 2023 4:55 PM
To: Banik, John (POL) <John.Banik@pol.state.ma.us>; Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
Cc: VOJNOVIC, DAMIR <DV289S@att.com>; DENNING, DONALD R <dd708h@att.com>; HAARDE, BOB <rh6158@att.com>
Subject: RE: Pilot- Final Data summary

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

Lt, Deb,

Good afternoon.

Please see attached Final Pilot Summary. Please let us know if you have any questions whatsoever or if you would like to review this information either in person or via a call.

I can also share the actual PPT slides if needed as well.

Have a great weekend!

Denis

Denis Lenehan II
Senior Principal Consultant, FirstNet Program
Public Safety Solutions

FirstNet.com

AT&T Mobility Services, Inc.
160 Federal St. 17th Floor Boston, MA 02110
☎: 617-306-9561 | ✉: dl009w@att.com

FIRSTNET. Built with AT&T

From: Banik, John (POL) <john.banik@state.ma.us>

Sent: Wednesday, February 15, 2023 2:05 PM
To: LENEHAN, DENIS R <dl009w@att.com>; DENNING, DONALD R <dd708h@att.com>
Cc: Connor, Debora (POL) <debora.connor@state.ma.us>
Subject: Pilot- Final Data summary

Good afternoon, in addition to any final reporting that you feel would be helpful to us we would like to see the following items:

1.) Overall data usage and broken down by troop for duration of pilot. (wi-fi vs cellular. Also if there is a breakdown of 5G vs LTE and by router type.)

2.) Aggregate map of the state for cellular connectivity for duration of pilot. Broken down by router.(we understand this may be limited due to lookback limitations)

3.) Amount of data transmitted via cellular specifically for CMC/BMC.

4.) Number of intakes to call center with time to resolution.

5.) HPUE usage overall and broken down by troop.

6.) Any possible info regarding the Hot Spot data usage?

7.) Any possible evidence of success in remote update / fix, or "application push" to the systems, cell phone and router? (I don't know if this is available, but may be nice to show remote fix capabilities)

8.) Pros/cons from vendor perspective of Sierra vs Cradlepoint and recommendation

9.) Pros/cons from vendor perspective of providing Help Desk support

10.) -Any possible info regarding the Hot Spot data usage?

11.) Any possible evidence of success in remote update / fix, or "application push" to the systems, cell phone and router? (I don't know if this is available, but may be nice to show remote fix capabilities)

12.)Any lessons learned each vendor would like to provide

Thank you,

Lt. John Banik #2947
Mass. State Police
Div. of Homeland Security and Preparedness

From: Foley, James (POL)
To: James Foley
Subject: Fw: POLICE TRAINING PROGRAM MATERIALS
Date: Thursday, February 9, 2023 12:32:43 AM
Attachments: Search Warrants for Digital Evidence (2.8.23) - PDF.pdf
Legal Process for Third Party Provider Data (2.8.23) - PDF.pdf
Legal Updates 2.8.23 - PDF.pdf
Drafting SW Affidavits 2.3.23 - PDF.pdf
2.8.23 SW Training_Search Warrant Process - PDF.pdf
2022-2023 Police Training Manual.pdf

Sergeant James J. Foley #2739
SP-Framingham/ H-2
450 Worcester Road
Framingham, MA 01702-2203
508-820-2250

From: Gouveia, Kim (NOR) <kim.gouveia@mass.gov>
Sent: Tuesday, February 7, 2023 3:23 PM
To: Foley, James (POL) <James.Foley@pol.state.ma.us>
Subject: POLICE TRAINING PROGRAM MATERIALS

Hello,

Attached please find the Police Training Materials. Thank you!

Kim Gouveia
Administrative Assistant to
Thomas D. Ralph, Chief Appeals & Training Bureau
Middlesex County District Attorney's Office
15 Commonwealth Avenue
Woburn, MA 01801
Phone: 781-897-6870
Fax: 781-897-6826

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: Foley, James (POL)
To: James Foley
Subject: Fw: POLICE TRAINING PROGRAM MATERIALS
Date: Saturday, February 11, 2023 4:49:00 PM
Attachments: Search Warrants for Digital Evidence (2.8.23) - PDF.pdf
Legal Process for Third Party Provider Data (2.8.23) - PDF.pdf
Legal Updates 2.8.23 - PDF.pdf
Drafting SW Affidavits 2.3.23 - PDF.pdf
2.8.23 SW Training_Search Warrant Process - PDF.pdf
2022-2023 Police Training Manual.pdf

Sergeant James J. Foley #2739
SP-Framingham/ H-2
450 Worcester Road
Framingham, MA 01702-2203
508-820-2250

From: Gouveia, Kim (NOR) <kim.gouveia@mass.gov>
Sent: Tuesday, February 7, 2023 3:23 PM
To: Foley, James (POL) <James.Foley@pol.state.ma.us>
Subject: POLICE TRAINING PROGRAM MATERIALS

Hello,

Attached please find the Police Training Materials. Thank you!

Kim Gouveia
Administrative Assistant to
Thomas D. Ralph, Chief Appeals & Training Bureau
Middlesex County District Attorney's Office
15 Commonwealth Avenue
Woburn, MA 01801
Phone: 781-897-6870
Fax: 781-897-6826

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: Salvatore, Justin (POL)
To: Lopez, Adrian (POL)
Subject: Fw: Reminder: Boss4
Date: Thursday, February 16, 2023 3:58:50 PM
Attachments: TRF-11 Automatic License Plate Recognition (1).pdf
image.png

Adrian,

Below is some guidance Sean sent out regarding the creation of Boss4 LPR hotlists. Just sending as FYI.

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: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Sent: Tuesday, January 24, 2023 6:54 AM
To: POL-DL-SPEAR <POL-DL-SPEAR@MassMail.State.MA.US>
Subject: Reminder: Boss4

Good Morning, All -

Just a reminder, please ensure that when entering hotlists into Boss4, we are all complying with the Department's ALPR policy (TRF-11, attached), as well as the additional recommendations regarding data retention (24-72 hour vs. 30 day hotlist entries). Sgt. Pack **does** perform routine audits of the ALPR system and hotlist entries, and has recently brought to my attention a handful of entries that do not comply with departmental policy.

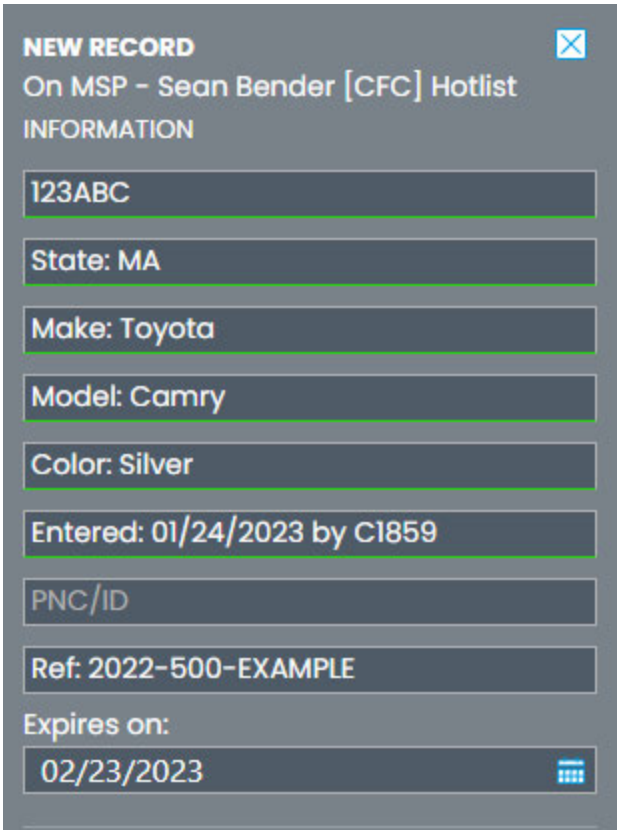
Minimum Requirements:

- Authorized purpose (refer to TRF-11)
  - *A case or reference number for a law enforcement investigation or legitimate public safety purpose is REQUIRED.*
- Update/Remove when information changes or is no longer current
  - 30 day expiration date for investigations, 24-72 hours for radio BOLOs, Dispatch requests, Public Safety hotlists etc. After the initial hotlist expires, the investigating officer is responsible for contacting the CFC for a longer term hotlist.
- Entered by:
  - Name or UserID of the user creating the hotlist, for audit purposes.

Additional Recommendations:

- State, Make, Model, Color
    - Including a physical description of the vehicle ensures that if a hit notification is received, recipients can confirm that the vehicle captured matches the suspect vehicle.
- Entered by (Date)
    - This helps us and the recipient to see how recent/relevant a hit notification may be. Agencies often forget to contact the CFC to remove the plate from the hotlist when it is no longer required.

In order to maintain compliance, uniformity, and consistency in our entries, I *highly* recommend utilizing the following format:



Please also ensure that when creating the notification profile that a hotlist is linked to the notification profile, otherwise, the plate may hit, but the user will not be notified. There are currently a number of notification profiles that are not linked to hotlists, or hotlists that are not linked to notification profiles. These hotlists will not function, even if the plate is captured by an ALPR device.

If you have any questions, please do not hesitate to reach out to myself, Justin, or Sgt. Pack.

Thank you.

Respectfully,

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

From: McCarthy, Daniel (AGO)
To: Morway, Timothy (POL); Bodreau, Jillian (AGO)
Subject: FW: Request - Massachusetts AGO
Date: Tuesday, June 20, 2023 5:32:30 PM
Attachments: LEARN_Vehicle_Detection_Report_06-20-23.pdf
LEARN_Vehicle_Detection_Report_06-20-23 (1).pdf
LEARN_Vehicle_Detection_Report_06-20-23 (2).pdf
3867_80a9a64cdd17456a958ce7ac3da8a594.pdf

Dan McCarthy
Sr. Intelligence Analyst
Enterprise and Major Crimes Division (EMCD)
New England Fentanyl Strike Force (NEFSF)
Office of the Attorney General
One Ashburton Place, 19th Floor
Boston, MA 02108
Cell: G.L. c. 4.sec. 7.cl.26 (n)(security)

From: NJSP ROIC WATCH <ROIC@njsp.gov>
Sent: Tuesday, June 20, 2023 4:51 PM
To: McCarthy, Daniel (AGO) <Daniel.J.McCarthy@mass.gov>
Subject: Re: Request - Massachusetts AGO

CAUTION: This email originated from a sender outside of the 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,

See attached. The plate has been hotlisted.

ROIC WATCH
G320 | Intelligence Watch and Warning Unit | The New Jersey Regional Operations & Intelligence Center | Main# 609-963-6951
ROIC@NJSP.GOV

From: McCarthy, Daniel J (AGO) <daniel.j.mccarthy@state.ma.us>
Sent: Tuesday, June 20, 2023 3:21 PM
To: NJSP ROIC WATCH <ROIC@njsp.gov>
Subject: [EXTERNAL] Request - Massachusetts AGO

*** CAUTION ***

This message came from an **EXTERNAL** address (Daniel.J.McCarthy@mass.gov). **DO NOT** click on links or attachments unless you know the sender and the content is safe.
New Jersey State Government Employees Should Forward Messages That May Be Cyber Security Risks To PhishReport@cyber.nj.gov.

Good Afternoon,

Pursuant to an active narcotics investigation by the Mass State Police and the MA Attorney General's

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

Trooper Stephen Durant
stephen.j.durant@pol.state.ma.us
Timothy Morway
timothy.morway@pol.state.ma.us
Daniel McCarthy
daniel.j.mccarthy@mass.gov
Jarred Matyka
jarred.m.matyka@ice.dhs.gov

Thank you!

Dan McCarthy
Sr. Intelligence Analyst
Enterprise and Major Crimes Division (EMCD)
New England Fentanyl Strike Force (NEFSF)
Office of the Attorney General
One Ashburton Place, 19th Floor
Boston, MA 02108
Cell: [redacted] G.L. c. 4.sec. 7.cl.26 (n)(security)

CONFIDENTIALITY NOTICE The information contained in this communication from the Office of the New Jersey Attorney General is privileged and confidential and is intended for the sole use of the

persons or entities who are the addressees. If you are not an intended recipient of this e-mail, the dissemination, distribution, copying or use of the information it contains is strictly prohibited. If you have received this communication in error, please immediately contact the Office of the Attorney General at (609) 292-4925 to arrange for the return of this information.

Subject: FW: Some flock camera materials
Date: Monday, February 6, 2023 4:39:51 PM
Attachments: A&O 13.16.2 LPRs.pdf
A&O 16.1.3 Selective Traffic Enforcement.pdf
A&O 16.6.1 Speed Monitoring.pdf
Executed LPR MOU Marlborough Nov 2021.pdf
ALPR Final.pdf
2019-118.pdf

Allison Hynes
Staff Legal Counsel
Office of Chief Legal Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Telephone: 508.820.2335

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: Ayers, Kathleen <Kathleen.Ayers@ct.gov>
Sent: Monday, February 6, 2023 4:20 PM
To: Hynes, Allison E (POL) <Allison.E.Hynes@pol.state.ma.us>
Subject: Some flock camera materials

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

… in case these aid in our discussion tomorrow. We call them LPRs (license plate readers)!

Thank you,

Kate Ayers
Staff Attorney 2
Department of Emergency Services and Public Protection
Phone: (860)-685-8150
Fax: (860)-685-8611
kathleen.ayers@ct.gov

NOTICE: This e-mail transmission and any accompanying attachments may contain confidential or privileged information. They are intended for use by the individual or entity named on this e-mail

transmission. If you are not the intended recipient, you are not authorized to disclose, copy, distribute or use, in any manner, the contents of this information. If you have received this e-mail transmission in error, please notify us by e-mail immediately.

From: Hynes, Allison E (POL)
To: Staples, Jennifer (POL); Brunelli, Daniel (POL)
Subject: FW: Some flock camera materials
Date: Monday, February 6, 2023 4:40:19 PM
Attachments: A&O 13.16.2 LPRs.pdf
A&O 16.1.3 Selective Traffic Enforcement.pdf
A&O 16.6.1 Speed Monitoring.pdf
Executed LPR MOU Marlborough Nov 2021.pdf
ALPR Final.pdf
2019-118.pdf

FYI

Allison Hynes
Staff Legal Counsel
Office of Chief Legal Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Telephone: 508.820.2335

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: Ayers, Kathleen <Kathleen.Ayers@ct.gov>
Sent: Monday, February 6, 2023 4:20 PM
To: Hynes, Allison E (POL) <Allison.E.Hynes@pol.state.ma.us>
Subject: Some flock camera materials

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

… in case these aid in our discussion tomorrow. We call them LPRs (license plate readers)!

Thank you,

Kate Ayers
Staff Attorney 2
Department of Emergency Services and Public Protection
Phone: (860)-685-8150
Fax: (860)-685-8611
kathleen.ayers@ct.gov

NOTICE: This e-mail transmission and any accompanying attachments may contain confidential or

privileged information. They are intended for use by the individual or entity named on this e-mail transmission. If you are not the intended recipient, you are not authorized to disclose, copy, distribute or use, in any manner, the contents of this information. If you have received this e-mail transmission in error, please notify us by e-mail immediately.

From: Fahey, Scott (POL)
To: Resendes, Eric (POL); Pacheco, Michael (POL)
Subject: Fw: TRF-11 Automatic License Plate Recognition
Date: Tuesday, June 27, 2023 7:07:35 PM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

From: Strategic Planning (POL) <strategic.planning@pol.State.MA.US>
Sent: Tuesday, June 27, 2023 2:04 PM
To: POL-DL-All Users <POL-DL-AllUsers@MassMail.State.MA.US>
Subject: TRF-11 Automatic License Plate Recognition

Please be advised that the following General Order has been promulgated and posted to PowerDMS. This is a revised version of TRF-11. Please use the comparison feature within PowerDMS to view the changes prior to signing off on the policy.

TRF-11 Automatic License Plate Recognition
PowerDMS location:
Documents
Policy and Procedure / Rules and Regulations
Policy and Procedure Documents
TRF-11

Strategic Planning and Analysis Section
Office of the Superintendent
470 Worcester Road
Framingham, MA 01702

From:	Teevens, Richard (POL)
To:	Collins, Barbara (POL); Convery, Michael (POL); Massa, Tania (POL); McDonough, John (POL); Rogers, Sade (POL); Saniuk, Michele (POL); Spychalski, Patricia (POL); Stephen, Camille C. (POL); Teevens, Richard (POL); Tilden, Charles (POL); Ward, Darryl (POL)
Subject:	Fw: TRF-11 Automatic License Plate Recognition
Date:	Tuesday, June 27, 2023 3:55:41 PM
Attachments:	TRF-11 Automatic License Plate Recognition.pdf

All,

Please read the updated policy regarding Automatic License Plate Readers then log into PowerDMS and sign off on the policy as soon as you can.

Thank you,

Richard E. Teevens
Massachusetts State Police
Public Safety Dispatcher II C309
Troop "H" Communications
617-946-3080 phone
617-946-0955 fax

From: Strategic Planning (POL) <strategic.planning@pol.State.MA.US>
Sent: Tuesday, June 27, 2023 2:04 PM
To: POL-DL-All Users <POL-DL-AllUsers@MassMail.State.MA.US>
Subject: TRF-11 Automatic License Plate Recognition

Please be advised that the following General Order has been promulgated and posted to PowerDMS. This is a revised version of TRF-11. Please use the comparison feature within PowerDMS to view the changes prior to signing off on the policy.

TRF-11 Automatic License Plate Recognition
PowerDMS location:
Documents
Policy and Procedure / Rules and Regulations
Policy and Procedure Documents
TRF-11

Strategic Planning and Analysis Section
Office of the Superintendent
470 Worcester Road
Framingham, MA 01702

From: Ryan, Robert (POL)
To: Pinkes, William (POL)
Subject: Fw: TRF-11 Automatic License Plate Recognition
Date: Monday, August 28, 2023 11:04:33 AM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

The below email was distributed to the department through PowerDMS which requires a signature. This is one of our criteria for Accreditation. Just wanted to make sure you had this information.

-Rob.

From: Strategic Planning (POL) <strategic.planning@pol.State.MA.US>
Sent: Tuesday, June 27, 2023 2:04 PM
To: POL-DL-All Users <POL-DL-AllUsers@MassMail.State.MA.US>
Subject: TRF-11 Automatic License Plate Recognition

Please be advised that the following General Order has been promulgated and posted to PowerDMS. This is a revised version of TRF-11. Please use the comparison feature within PowerDMS to view the changes prior to signing off on the policy.

TRF-11 Automatic License Plate Recognition
PowerDMS location:
Documents
Policy and Procedure / Rules and Regulations
Policy and Procedure Documents
TRF-11

Strategic Planning and Analysis Section
Office of the Superintendent
470 Worcester Road
Framingham, MA 01702

From: Nunes, John (POL)
To: DaSilva, Kelsey (POL)
Subject: FW: TSU ALPR SGT
Date: Monday, July 17, 2023 2:46:00 PM
Attachments: TSU SGT APLR Full Packet.pdf
TSU Sgt Posting questions interview and selection Jul 2023.docx
Outlook-1xre1d1i.png
image001.png

Respectfully,
Detective Captain John B. Nunes #2426
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd.
Framingham, MA 01702
(W) 508-988-7312
(C) 508-245-2984
john.nunes@pol.state.ma.us



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 message in error, please delete this email immediately.

From: Grasso, Jimi (POL) <jimi.grasso@pol.state.ma.us>
Sent: Wednesday, July 12, 2023 11:19 AM
To: George, Michael (POL) <Michael.George@pol.state.ma.us>; Nunes, John (POL) <john.nunes@pol.state.ma.us>
Cc: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Subject: Re: TSU ALPR SGT

Thank you!

Respectfully submitted,

Major Jimi Grasso #2529

Massachusetts State Police

Division of Homeland Security and Preparedness

470 Worcester Road Framingham, MA 01702

(office) 508-820-2661 / (mobile) 5[M.G.L. c. 4 sec. 7 cl.26 (n)(security)]



Information contained in this email may be confidential and/or CORI. Receipt and/or dissemination by persons other than the intended addressee may be subject to criminal penalties.

From: George, Michael (POL) <Michael.George@pol.state.ma.us>
Sent: Wednesday, July 12, 2023 11:07 AM
To: Grasso, Jimi (POL) <jimi.grasso@pol.state.ma.us>; Nunes, John (POL) <john.nunes@pol.state.ma.us>
Subject: TSU ALPR SGT

Sirs,
See attached RE TSU ALPR SGT Selection

Respectfully,

Lieutenant Michael A. George #2998
Massachusetts State Police
Division of Homeland Security and Preparedness
Technical Services Unit
21 Oak St
Leominster, MA 01453
michael.george@pol.state.ma.us
Personal Cell: [M.G.L. c. 4 sec. 7 cl.26 (n)(security)]

Technical Services Satellite Office
136 Washington Street
Foxboro, MA 02035

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.

All communications sent or received by this Commonwealth of Massachusetts email address may be subject to disclosure under the Massachusetts Public Records Law (M.G.L. Chapter 66, Section 10) and the Federal Freedom of Information Act.

Subject: FW: Utilization of Video Systems in the CWC
Date: Friday, April 7, 2023 8:23:30 AM
Attachments: image001.png
image002.png
CFC-12 Utilization of Video Systems in the Commonwealth Watch Center (DRAFT - template) - 04.04.23.docx

From: Stelmat, Jason (POL)
To: Thibault, Amy (POL)
Subject: FW: Utilization of Video Systems in the CWC
Date: Tuesday, April 4, 2023 3:05:42 PM
Attachments: image001.png
image002.png
CFC-12 Utilization of Video Systems in the Commonwealth Watch Center (DRAFT - template) - 04.04.23.docx

---

Amy,
Here is a draft version on the CFC policy template.

From: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Sent: Tuesday, April 4, 2023 10:37 AM
To: Stelmat, Jason (POL) <Jason.Stelmat@pol.state.ma.us>
Cc: Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>; Rudolph, James (POL) <James.Rudolph@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Subject: Re: Utilization of Video Systems in the CWC

Thank you, Jason. I appreciate the help and all the work on this.

Lieutenant Colonel Mark D. Cyr #2728
Massachusetts State Police
Division Commander
Division of Homeland Security and Preparedness
508-988-7301 (office)
[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: Stelmat, Jason (POL) <Jason.Stelmat@pol.state.ma.us>
Sent: Tuesday, April 4, 2023 10:32 AM
To: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Cc: Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>; Rudolph, James (POL) <James.Rudolph@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Subject: RE: Utilization of Video Systems in the CWC

Col. Cyr,
I've incorporated the changes for your review. I'm attaching both the tracked changes and clean versions for reference.

Let us know how we can further assist.

Best,
Jason

From: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Sent: Friday, March 31, 2023 9:59 PM
To: Stelmat, Jason (POL) <Jason.Stelmat@pol.state.ma.us>
Cc: Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>; Rudolph, James (POL) <James.Rudolph@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Subject: Re: Utilization of Video Systems in the CWC

Thank you, Jason. These should be the final edits! Please incorporate your suggested changes and forward the draft. I will send it to Mike Halpin for one final Legal review before we post it in the Watch.

I appreciate all the work you and Amy have put into this.

Mark

Lieutenant Colonel Mark D. Cyr #2728
Massachusetts State Police
Division Commander
Division of Homeland Security and Preparedness
508-988-7301 (office)
G.L. c. 4,sec. 7,cl.26 (n)(security) *(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: Stelmat, Jason (POL) <Jason.Stelmat@pol.state.ma.us>
Sent: Friday, March 31, 2023 3:33 PM
To: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Cc: Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>; Rudolph, James (POL) <James.Rudolph@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Subject: RE: Utilization of Video Systems in the CWC

Col. Cyr,
Amy and I have reviewed the most recent draft. We noticed the term "systems" was removed from a few of the sections but still remains in other sections, including the title. For consistency purposes, we would recommend reinserting the term where it was removed or removing it from the policy altogether.

With respect to Cpt. Rudolph's suggestions:

(1) We agree with adding "and Security" to the EOPSS reference in the Grant Provision definition.

(2) Changing “are” to “is” would be appropriate of we remove the term “systems” from these sections. If we reinstert the term, it should remain “are.”
(3) With respect to the comma after the term “video,” we believe it should be left out so as to preserve “video data” as a single term.

I’d be happy to incorporate these suggestions into a new draft if you think it would be helpful.

Have a great weekend.

-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

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. Thank-you.

Please consider the environment before printing this e-mail

From: Rudolph, James (POL) <James.Rudolph@pol.state.ma.us>
Sent: Saturday, March 25, 2023 11:20 AM
To: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Stelmat, Jason (POL) <Jason.Stelmat@pol.state.ma.us>
Cc: Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>
Subject: Re: Utilization of Video Systems in the CWC

I won't fool anyone into thinking I can judge the subject matter, but strictly from a proofreading standpoint if someone could please review the following 3 items in red:

1.) In the "Definition" section, I believe a couple words might have been inadvertently left out of the Grant Provisions bullet:

> *Grant Provisions*: *The provisions of the U.S. Department of Homeland Security / Federal Emergency Management Agency Port Security Grant (Sub Account No. EMW-*

*2020-PU-0056) awarded to the Massachusetts Executive Office of Public Safety **and Security** (EOPSS), effective on July 1, 2022, and any/all subsequent related grants or award(s).*

2.) In the section, "Authorized Access and Uses" (A and B) should it be "is" instead of "are" in these spots? I am not a grammar expert so feel free to tell me I'm wrong.

A. *Access to video viewable at the Commonwealth Watch Center that **are** not available to the general public shall be restricted to authorized Watch Center employees, Fusion Center employees, Department employees with Watch Center access, and other individuals authorized by the Commonwealth Watch Center supervisor, Fusion Center Commander, Division Commanders, or the Colonel or designee.*

*B. Use of video viewable at the Commonwealth Watch Center video **are** strictly limited...*

3.) In the Section "Prosecutorial & Court Ordered Restrictions" should there be a comma after "video"?

Commonwealth Watch Center video, data, and information are subject to state and federal laws...

Thank you,
-Jim

RESPECTFULLY,

CAPTAIN JAMES D. RUDOLPH #2786
EXECUTIVE OFFICER, DIVISION OF STANDARDS AND TRAINING
MASSACHUSETTS STATE POLICE
470 WORCESTER ROAD, FRAMINGHAM, MA 01702
508-820-2132

From: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Sent: Saturday, March 25, 2023 9:07 AM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Stelmat, Jason (POL) <Jason.Stelmat@pol.state.ma.us>

Cc: Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>; Rudolph, James (POL) <James.Rudolph@pol.state.ma.us>
Subject: Utilization of Video Systems in the CWC

Amy and Jason,
Attached, find the most recent draft of the Watch "Utilization of Video Systems in the Commonwealth Watch Center." There have been changes since the last review. I think we are very close. Please review and reach out with any questions/concerns. Thank you for all the hard work on this.

Lieutenant Colonel Mark D. Cyr #2728
Massachusetts State Police
Division Commander
Division of Homeland Security and Preparedness
508-988-7301 (office)
[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: Stelmat, Jason (POL)
To: Thibault, Amy (POL)
Subject: FW: Utilization of Video Systems in the CWC
Date: Tuesday, March 28, 2023 10:19:35 AM
Attachments: Outlook-jrecu53b.png
Utilization of Video Systems in the Commonwealth Watch Center (DRAFT) (highlighted changes JRS).docx
Commonwealth Watch Center Video Systems Policy (DRAFT) - JRS 01.06.23.docx

---

Amy,
I've highlighted Col. Cyr's latest draft to show the changes that were made since we submitted our draft in January. Both documents are attached for reference.

Regarding D. Capt. Rudolph's suggestions:

(1) Agree
(2) Given that they've removed the word "systems" from those paragraphs, I would agree to change "are" to "is."
(3) I would disagree with adding the comma. I believe "video data" should be its own term.

From: Rudolph, James (POL) <James.Rudolph@pol.state.ma.us>
Sent: Saturday, March 25, 2023 11:20 AM
To: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Stelmat, Jason (POL) <Jason.Stelmat@pol.state.ma.us>
Cc: Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>
Subject: Re: Utilization of Video Systems in the CWC

I won't fool anyone into thinking I can judge the subject matter, but strictly from a proofreading standpoint if someone could please review the following 3 items in red:

1.) In the "Definition" section, I believe a couple words might have been inadvertently left out of the Grant Provisions bullet:

> *Grant Provisions*: *The provisions of the U.S. Department of Homeland Security / Federal Emergency Management Agency Port Security Grant (Sub Account No. EMW-2020-PU-0056) awarded to the Massachusetts Executive Office of Public Safety* ***and Security*** *(EOPSS), effective on July 1, 2022, and any/all subsequent related grants or award(s).*

2.) In the section, "Authorized Access and Uses" (A and B) should it be "is" instead of "are" in these spots? I am not a grammar expert so feel free to tell me I'm wrong.

A. *Access to video viewable at the Commonwealth Watch Center that* ***are*** *not available to the general public shall be restricted to authorized Watch Center employees, Fusion Center employees, Department employees with Watch Center access, and other individuals authorized*

by the Commonwealth Watch Center supervisor, Fusion Center Commander, Division Commanders, or the Colonel or designee.

*B. Use of video viewable at the Commonwealth Watch Center video **are** strictly limited...*

3.) In the Section "Prosecutorial & Court Ordered Restrictions" should there be a comma after "video"?

> *Commonwealth Watch Center video, data, and information are subject to state and federal laws...*

Thank you,
-Jim

RESPECTFULLY,

CAPTAIN JAMES D. RUDOLPH #2786
EXECUTIVE OFFICER, DIVISION OF STANDARDS AND TRAINING
MASSACHUSETTS STATE POLICE
470 WORCESTER ROAD, FRAMINGHAM, MA 01702
508-820-2132

From: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Sent: Saturday, March 25, 2023 9:07 AM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Stelmat, Jason (POL) <Jason.Stelmat@pol.state.ma.us>
Cc: Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>; Rudolph, James (POL) <James.Rudolph@pol.state.ma.us>
Subject: Utilization of Video Systems in the CWC

Amy and Jason,
Attached, find the most recent draft of the Watch "Utilization of Video Systems in the Commonwealth Watch Center." There have been changes since the last review. I think we are very close. Please review and reach out with any questions/concerns. Thank you for all the hard work on this.

Lieutenant Colonel Mark D. Cyr #2728

Massachusetts State Police
Division Commander
Division of Homeland Security and Preparedness
508-988-7301 (office)
G.L. c. 4,sec. 7,cl.26 (n)(security) *(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: Thibault, Amy (POL)
To: Tucker, Daniel T (POL)
Cc: Stelmat, Jason (POL)
Subject: FW: Utilization of Video Systems in the CWC
Date: Friday, April 7, 2023 8:25:00 AM
Attachments: image001.png
image002.png
CFC-12 Utilization of Video Systems in the Commonwealth Watch Center (DRAFT - template) - 04.04.23.docx

---

Good morning Major Tucker,
LTC Cyr requested that Jason formalize this video policy as a CFC policy. It has been approved by legal. As the fusion center director, you are the authority for CFC policies. Please sign the policy and then we can have all personnel sign off that they have read and understand the policy.

Thank you,
Amy

From: Stelmat, Jason (POL) <Jason.Stelmat@pol.state.ma.us>
Sent: Tuesday, April 4, 2023 3:06 PM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Subject: FW: Utilization of Video Systems in the CWC

Amy,
Here is a draft version on the CFC policy template.

From: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Sent: Tuesday, April 4, 2023 10:37 AM
To: Stelmat, Jason (POL) <Jason.Stelmat@pol.state.ma.us>
Cc: Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>; Rudolph, James (POL) <James.Rudolph@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Subject: Re: Utilization of Video Systems in the CWC

Thank you, Jason. I appreciate the help and all the work on this.

Lieutenant Colonel Mark D. Cyr #2728

Massachusetts State Police

Division Commander

Division of Homeland Security and Preparedness

508-988-7301 (office)

[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: Stelmat, Jason (POL) <Jason.Stelmat@pol.state.ma.us>
Sent: Tuesday, April 4, 2023 10:32 AM
To: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Cc: Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>; Rudolph, James (POL) <James.Rudolph@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Subject: RE: Utilization of Video Systems in the CWC

Col. Cyr,
I've incorporated the changes for your review. I'm attaching both the tracked changes and clean versions for reference.

Let us know how we can further assist.

Best,
Jason

From: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Sent: Friday, March 31, 2023 9:59 PM
To: Stelmat, Jason (POL) <Jason.Stelmat@pol.state.ma.us>
Cc: Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>; Rudolph, James (POL) <James.Rudolph@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Subject: Re: Utilization of Video Systems in the CWC

Thank you, Jason. These should be the final edits! Please incorporate your suggested changes and forward the draft. I will send it to Mike Halpin for one final Legal review before we post it in the Watch.

I appreciate all the work you and Amy have put into this.

Mark

Lieutenant Colonel Mark D. Cyr #2728

Massachusetts State Police

Division Commander

Division of Homeland Security and Preparedness

508-988-7301 (office)

[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: Stelmat, Jason (POL) <Jason.Stelmat@pol.state.ma.us>
Sent: Friday, March 31, 2023 3:33 PM
To: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Cc: Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>; Rudolph, James (POL) <James.Rudolph@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Subject: RE: Utilization of Video Systems in the CWC

Col. Cyr,
Amy and I have reviewed the most recent draft. We noticed the term "systems" was removed from a few of the sections but still remains in other sections, including the title. For consistency purposes, we would recommend reinserting the term where it was removed or removing it from the policy altogether.

With respect to Cpt. Rudolph's suggestions:

(1) We agree with adding "and Security" to the EOPSS reference in the Grant Provision definition.
(2) Changing "are" to "is" would be appropriate of we remove the term "systems" from these sections. If we reinstert the term, it should remain "are."
(3) With respect to the comma after the term "video," we believe it should be left out so as to preserve "video data" as a single term.

I'd be happy to incorporate these suggestions into a new draft if you think it would be helpful.

Have a great weekend.

-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

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. Thank-you.

Please consider the environment before printing this e-mail

From: Rudolph, James (POL) <James.Rudolph@pol.state.ma.us>
Sent: Saturday, March 25, 2023 11:20 AM
To: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Stelmat, Jason (POL) <Jason.Stelmat@pol.state.ma.us>
Cc: Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>
Subject: Re: Utilization of Video Systems in the CWC

I won't fool anyone into thinking I can judge the subject matter, but strictly from a proofreading standpoint if someone could please review the following 3 items in red:

1.) In the "Definition" section, I believe a couple words might have been inadvertently left out of the Grant Provisions bullet:

> *Grant Provisions*: *The provisions of the U.S. Department of Homeland Security / Federal Emergency Management Agency Port Security Grant (Sub Account No. EMW-2020-PU-0056) awarded to the Massachusetts Executive Office of Public Safety* ***and Security*** *(EOPSS), effective on July 1, 2022, and any/all subsequent related grants or award(s).*

2.) In the section, "Authorized Access and Uses" (A and B) should it be "is" instead of "are" in these spots? I am not a grammar expert so feel free to tell me I'm wrong.

A. *Access to video viewable at the Commonwealth Watch Center that* ***are*** *not available to the general public shall be restricted to authorized Watch Center employees, Fusion Center employees, Department employees with Watch Center access, and other individuals authorized by the Commonwealth Watch Center supervisor, Fusion Center Commander, Division Commanders, or the Colonel or designee.*

B. Use of video viewable at the Commonwealth Watch Center video ***are*** *strictly limited...*

3.) In the Section "Prosecutorial & Court Ordered Restrictions" should there be a comma after "video"?

> *Commonwealth Watch Center video, data, and information are subject to state and federal laws...*

Thank you,
-Jim

Respectfully,

Captain James D. Rudolph #2786
Executive Officer, Division of Standards and Training
Massachusetts State Police
470 Worcester Road, Framingham, MA 01702
508-820-2132

From: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Sent: Saturday, March 25, 2023 9:07 AM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Stelmat, Jason (POL) <Jason.Stelmat@pol.state.ma.us>
Cc: Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>; Rudolph, James (POL) <James.Rudolph@pol.state.ma.us>
Subject: Utilization of Video Systems in the CWC

Amy and Jason,
Attached, find the most recent draft of the Watch "Utilization of Video Systems in the Commonwealth Watch Center." There have been changes since the last review. I think we

are very close. Please review and reach out with any questions/concerns. Thank you for all the hard work on this.

Lieutenant Colonel Mark D. Cyr #2728

Massachusetts State Police

Division Commander

Division of Homeland Security and Preparedness

508-988-7301 (office)

[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: Bender, Sean (POL)
To: Peterson, Kaitlyn H. (POL)
Subject: Fw: Vigilant LPR Follow Up
Date: Friday, September 15, 2023 7:08:11 AM
Attachments: Adding New Hot Plates.pdf
Accessing Vigilant On-Demand Training.pdf
Customizing QuickSearch View.pdf
Locate Analysis.pdf
Open Source Free Internet Sites.xlsx
My Profile - Configuring Alert Management (1).pdf
Open Source-Online Resources.pdf
Vigilant Training Team.pdf
Vigilant PlateSearch Active Hit Protocol Guidelines (1).pdf
Stakeout.pdf
Wild Card Help.pdf
AAMVA-LicensePlateReaderProgramBestPracticesGuide-October2021.pdf
MCCA-Automated-License-Plate-Reader-Technology-in-Law-Enforcement.pdf
LPR Class Roster-MSP-09142023.xlsx

From: Christopher Scandole <christopher scandole@motorolasolutions.com>
Sent: Friday, September 15, 2023 5:35 AM
Subject: Vigilant LPR 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.

Good Morning All,

It was an absolute pleasure meeting you all at the training session yesterday, and truly a privilege and honor to spend some time in the Bay State, among active members of the Massachusetts State Police. See the attachments to this email for some quick help references and free internet resources, to assist in your searches. The class roster is also attached, we encourage you to network with each other.

The below links are for our training site and for the On-Demand training.

https://vslea.org/

https://vigilant.policeoneacademy.com/login/#login

For Info on Commercial scans and for Certified Copies of Search results for court, send an email to VigilantRecords@MotorolaSolutions.com

For Case Assistance send an email to VigilantTraining@MotorolaSolutions.com

To request access to EPIC use this link - https://esp.usdoj.gov/nur/

Please feel free to reach out to the training team with any questions, and as always please stay safe and be careful out there

Chris

Chris Scandole
Manager, Customer Training & Development
Detective 1st Grade, NYPD (Retired)
Video Security & Analytics
Vigilant

m: +1.917.913 3351
Training: **www.vslea.org**
Case Assistance: **VigilantTraining@motorolasolutions.com**

CLICK HERE TO SCHEDULE AGENCY MANAGER TRAINING

CLICK HERE TO SCHEDULE END-USER TRAINING

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

From: Franquiz, Andrew (POL)
To: Lopez, Adrian (POL)
Subject: Fw: Vigilant LPR Follow Up
Date: Tuesday, October 24, 2023 10:24:02 PM
Attachments: Adding New Hot Plates.pdf
Accessing Vigilant On-Demand Training.pdf
Customizing QuickSearch View.pdf
Locate Analysis.pdf
Open Source Free Internet Sites.xlsx
My Profile - Configuring Alert Management (1).pdf
Open Source-Online Resources.pdf
Vigilant Training Team.pdf
Vigilant PlateSearch Active Hit Protocol Guidelines (1).pdf
Stakeout.pdf
Wild Card Help.pdf
AAMVA-LicensePlateReaderProgramBestPracticesGuide-October2021.pdf
MCCA-Automated-License-Plate-Reader-Technology-in-Law-Enforcement.pdf
LPR Class Roster-MSP-09142023.xlsx

From: Christopher Scandole <christopher scandole@motorolasolutions.com>
Sent: Friday, September 15, 2023 5:35 AM
Subject: Vigilant LPR 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.

Good Morning All,

It was an absolute pleasure meeting you all at the training session yesterday, and truly a privilege and honor to spend some time in the Bay State, among active members of the Massachusetts State Police. See the attachments to this email for some quick help references and free internet resources, to assist in your searches. The class roster is also attached, we encourage you to network with each other.

The below links are for our training site and for the On-Demand training.

https://vslea.org/

https://vigilant.policeoneacademy.com/login/#login

For Info on Commercial scans and for Certified Copies of Search results for court, send an email to VigilantRecords@MotorolaSolutions.com

For Case Assistance send an email to VigilantTraining@MotorolaSolutions.com

To request access to EPIC use this link - https://esp.usdoj.gov/nur/

Please feel free to reach out to the training team with any questions, and as always please stay safe and be careful out there

Chris

Chris Scandole
Manager, Customer Training & Development
Detective 1st Grade, NYPD (Retired)
Video Security & Analytics
Vigilant

m: +1.917.913 3351
Training: **www.vslea.org**
Case Assistance: **VigilantTraining@motorolasolutions.com**

CLICK HERE TO SCHEDULE AGENCY MANAGER TRAINING

CLICK HERE TO SCHEDULE END-USER TRAINING

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

From: sean.maher@pol.state.ma.us
To: Jones, Liam (WES)
Subject: Fwd: ALPR Policy Update
Date: Saturday, July 1, 2023 10:55:50 PM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

Sent from my iPhone

Begin forwarded message:

From: "Pack, Noah (POL)" <noah.pack@pol.state.ma.us>
Date: July 1, 2023 at 9:07:36 PM EDT
To: "Pack, Noah (POL)" <noah.pack@pol.state.ma.us>
Subject: ALPR Policy Update

Notification of ALPR Policy Update

The Department's ALPR policy (TRF-11) was officially updated as of June 27, 2023. An updated copy is attached to this email. This policy governs the use of the ALPR systems by sworn and civilian members of MSP. Please review it to ensure you are familiar with the most recent version. Many of the updates directly reflect the best practices that we have already been using and teaching, such as limiting the scope of searches and the duration of manual hotlist entries.

One noteworthy update is that a manual hotlist entry request must be authorized by a supervisor, except in exigent circumstances/emergencies. This can be satisfied in one of two ways: (1) the request can come directly from a supervisor (Sgt. or above or civilian equivalent), or (2) the requestor can provide the name of the supervisor who has authorized the request. If you or a member of your unit submits a hotlist request to the Watch Center, they will respond with an inquiry about this authorization if it does not meet one of those criteria in the initial request.

As always please feel free to reach out with questions, comments, or success stories.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

From: Maher, Sean (POL)
To: Jones, Liam (WES)
Subject: Fwd: ALPR Policy Update
Date: Saturday, July 1, 2023 10:55:52 PM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

Sent from my iPhone

Begin forwarded message:

From: "Pack, Noah (POL)" <noah.pack@pol.state.ma.us>
Date: July 1, 2023 at 9:07:36 PM EDT
To: "Pack, Noah (POL)" <noah.pack@pol.state.ma.us>
Subject: ALPR Policy Update

Notification of ALPR Policy Update

The Department's ALPR policy (TRF-11) was officially updated as of June 27, 2023. An updated copy is attached to this email. This policy governs the use of the ALPR systems by sworn and civilian members of MSP. Please review it to ensure you are familiar with the most recent version. Many of the updates directly reflect the best practices that we have already been using and teaching, such as limiting the scope of searches and the duration of manual hotlist entries.

One noteworthy update is that a manual hotlist entry request must be authorized by a supervisor, except in exigent circumstances/emergencies. This can be satisfied in one of two ways: (1) the request can come directly from a supervisor (Sgt. or above or civilian equivalent), or (2) the requestor can provide the name of the supervisor who has authorized the request. If you or a member of your unit submits a hotlist request to the Watch Center, they will respond with an inquiry about this authorization if it does not meet one of those criteria in the initial request.

As always please feel free to reach out with questions, comments, or success stories.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

From: Benson, Eric (POL)
To: Morris, Samantha (POL)
Subject: Fwd: Flock ALPR_VFAS
Date: Friday, August 4, 2023 1:28:09 PM
Attachments: Flock_To_From.doc

Sam,

Please see attached request.

Respectfully,

Detective Captain Eric J. Benson, #3389
Massachusetts State Police
Division of Investigative Services
470 Worcester Road
Framingham, MA 01702
(508) 525-5988

From: Sullivan, John (POL) <john.sullivan@pol.state.ma.us>
Sent: Friday, August 4, 2023 1:16:22 PM
To: Connors, Brian (POL) <Brian.Connors@pol.state.ma.us>; Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>; Farley, Michael (POL) <michael.farley@pol.state.ma.us>; Benson, Eric (POL) <Eric.J.Benson@pol.state.ma.us>
Cc: Banik, John (POL) <John.Banik@pol.state.ma.us>
Subject: Flock ALPR_VFAS

Please see attached To/From. Respectfully,

Sully

Detective Lieutenant John B. Sullivan #3359
Massachusetts State Police
Unit Commander
Violent Fugitive Apprehension Section
Office: 508-820-2374
Cell: [redacted]

From: Pack, Noah (POL)
To: Cyr, Mark (POL); Walczak, Ryan (POL)
Subject: Fwd: LPR success story
Date: Tuesday, July 25, 2023 12:38:09 PM
Attachments: image004.png

LTC Cyr:

Please see the below message from Barnstable PD regarding a successful outcome to a serious felony incident that highlights the community benefits of our LPR program and our ongoing support, training, and collaboration with partner agencies across the Commonwealth.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Investigative Services
Critical Incident Technical Investigations (CITI)

From: Connolly, Kevin <connollyk@barnstablepolice.com>
Sent: Tuesday, July 25, 2023 12:30
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: LPR success story

CAUTION: This email originated from a sender outside of the 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 just wanted to pass along a quick success story we had here in Barnstable. On May 27, 2023 we had 2 unknown individuals fire several rounds at a motor vehicle in the Craigville Beach parking lot at 8:30pm as beachgoers were in the area enjoying a nice sunset. Although no one was hit, the vehicle was struck 5 times and the community was immediately put on edge because of this brazen violent act.

As we were developing suspects we were able to identify the vehicle and plate of the car used to help the shooters flee the scene. Utilizing CSLI for the suspected occupants and plate reads from Yarmouth, Barnstable, and Sagamore we were able to show the vehicle and the suspects traveling together prior to and immediately after the shooting. Having access to the plate readers in the other communities was invaluable in this investigation and helped solidify the probable cause needed to obtain arrest warrants for the responsible parties.

Thank you again for keeping these readers up and running, they truly help more than you know.

Kevin

Kevin A. Connolly
Detective Sergeant
Barnstable Police Department
Investigative Services Division
Digital Forensics & Investigations Unit
USSS New England Cyber Fraud Task Force
508-958-6522
connollyk@barnstablepolice.com

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Saturday, July 1, 2023 8:50 PM
To: Pack, Noah (POL) <noah.pack@state.ma.us>
Subject: LPR System User Updates

[EXTERNAL EMAIL] DO NOT CLICK links or attachments unless you recognize the sender and know the content is safe.

CAUTION: This email originated from outside your organization. Exercise caution when opening attachments or clicking links, especially from unknown senders.

Hello Boss4 users, please see the updates below regarding the Department's ALPR system.

Policy Update

The Department's ALPR policy (TRF-11) was officially updated as of June 27, 2023. An updated copy is attached to this email. This policy governs the use of the Department's ALPR systems by sworn and civilian members of MSP and our partner agencies who have completed MOUs with us. Please review it to ensure you are familiar with the most recent version. Many of the updates to this policy directly reflect the best practices that we have already been doing and teaching, such as limiting the scope of searches and the duration of manual hotlist entries.

One noteworthy update is that a manual hotlist entry request must be authorized by a supervisor, except in exigent circumstances/emergencies. This can be satisfied in one of two ways: (1) the request can come directly from a supervisor (Sgt. or above or civilian equivalent), or (2) the requestor can provide the name of the supervisor who has authorized the request.

Hotlist Entries

When entering a plate on a hotlist, information must be entered in the free text fields about the vehicle, the reason for the entry, the date of the entry, and who entered it. Please do not enter just a plate. For investigations, include enough information to identify what vehicle and case it refers to. For public safety entries, include enough info so that someone receiving the alert would know what to do or who to call if it alerts them. For all entries, there must be enough info so that we can identify an authorized use and specific case or incident when conducting an audit. An example of a solid entry would be:

LPN: 123ABC
Field 1: 2020
Field 2: Toyota
Field 3: Highlander
Field 4: White
Field 5: Entered 5/1/23 by #1234
Field 6: Homicide invest [OR] New Bedford kidnapping
Field 7: 2023-123-123 [OR] Contact New Bedford PD

Expiration dates: Manual hotlist entries must have an initial expiration date of no longer than 30 days and must be removed as soon as the information become invalid or is no longer needed for the investigation. For entries requested by a dispatch entity or for other short-term matters, such as a general BOLO, the entries must be set to expire no later than the following day (generally 24-48 hours). The intent of this is to avoid a plate being left on the hotlist for long after the short-term incident is resolved.

Searches:

When conducting a search, please be mindful of the temporal and geographic parameters that are reasonable and consistent with the needs of the investigation or incident. In short, this means to ask how much historical time and how much area (how many cameras) do we need to search, as these are among the questions being asked in court when assessing the reasonableness of LPR use in a particular case.

Historical data visibility is currently limited to **90 days**, but data is retained for 1 year by DCJIS policy. If you need to search further back than 90 days, please contact the Commonwealth Watch Center for assistance at fusion@mass.gov.

Successes:

LPR continues to provide critical information for major incidents and investigations, from shootings to kidnappings, all over the Commonwealth. Please continue to forward these

success stories to me or the Watch Center to help us document and defend the public safety value of this system. Feel free to also forward any suggestions on how we might improve the system.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

From: Ferguson, Gary E (POL)
To: Neville, Christopher (POL)
Subject: Fwd: TRF-11 Automatic License Plate Recognition
Date: Tuesday, June 27, 2023 3:02:27 PM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

From: Strategic Planning (POL) <strategic.planning@pol.State.MA.US>
Sent: Tuesday, June 27, 2023 2:04:28 PM
To: POL-DL-All Users <POL-DL-AllUsers@MassMail.State.MA.US>
Subject: TRF-11 Automatic License Plate Recognition

Please be advised that the following General Order has been promulgated and posted to PowerDMS. This is a revised version of TRF-11. Please use the comparison feature within PowerDMS to view the changes prior to signing off on the policy.

TRF-11 Automatic License Plate Recognition
PowerDMS location:
Documents
Policy and Procedure / Rules and Regulations
Policy and Procedure Documents
TRF-11

Strategic Planning and Analysis Section
Office of the Superintendent
470 Worcester Road
Framingham, MA 01702

From: Adrian Lopez
To: Lopez, Adrian (POL)
Subject: Fwd: Vigilant LPR Follow Up
Date: Friday, September 15, 2023 3:32:36 PM
Attachments: Adding New Hot Plates.pdf
Accessing Vigilant On-Demand Training.pdf
Customizing QuickSearch View.pdf
Locate Analysis.pdf
Open Source Free Internet Sites.xlsx
My Profile - Configuring Alert Management (1).pdf
Open Source-Online Resources.pdf
Vigilant Training Team.pdf
Vigilant PlateSearch Active Hit Protocol Guidelines (1).pdf
Stakeout.pdf
Wild Card Help.pdf
AAMVA-LicensePlateReaderProgramBestPracticesGuide-October2021.pdf
MCCA-Automated-License-Plate-Reader-Technology-in-Law-Enforcement.pdf
LPR Class Roster-MSP-09142023.xlsx

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

---------- Forwarded message ---------
From: **Christopher Scandole** <christopher.scandole@motorolasolutions.com>
Date: Fri, Sep 15, 2023, 5:37 AM
Subject: Vigilant LPR Follow Up
To:

Good Morning All,

It was an absolute pleasure meeting you all at the training session yesterday, and truly a privilege and honor to spend some time in the Bay State, among active members of the Massachusetts State Police. See the attachments to this email for some quick help references and free internet resources, to assist in your searches. The class roster is also attached, we encourage you to network with each other.

The below links are for our training site and for the On-Demand training.

https://vslea.org/

https://vigilant.policeoneacademy.com/login/#login

For Info on Commercial scans and for Certified Copies of Search results for court, send an email to VigilantRecords@MotorolaSolutions.com

For Case Assistance send an email to VigilantTraining@MotorolaSolutions.com

To request access to EPIC use this link - https://esp.usdoj.gov/nur/

Please feel free to reach out to the training team with any questions, and as always please stay safe and be careful out there

Chris

Chris Scandole
Manager, Customer Training & Development
Detective 1st Grade, NYPD (Retired)
Video Security & Analytics
Vigilant

m: +1.917.913 3351

Training: **www.vslea.org**

Case Assistance: **VigilantTraining@motorolasolutions.com**

CLICK HERE TO SCHEDULE AGENCY MANAGER TRAINING

CLICK HERE TO SCHEDULE END-USER TRAINING

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

From: Walczak, Ryan (POL)
To: Cyr, Mark (POL)
Cc: Pack, Noah (POL)
Subject: FYI
Date: Tuesday, September 5, 2023 2:02:15 PM
Attachments: DRAFT for Review(1).docx

Good Afternoon LTC,
Please see attached for your review.

Respectfully,
Ryan

Sergeant Ryan Walczak #3731
Massachusetts State Police
Division Of Homeland Security and Preparedness
Technical Services Unit
Cell # [redacted] M.G.L. c. 4 sec. 7 cl 26 (n)(security)
Email: Ryan.walczak@pol.state.ma.us

From: Cyr, Mark (POL)
To: Pack, Noah (POL)
Subject: FYI
Date: Wednesday, September 6, 2023 3:16:21 PM
Attachments: ALPR Div Comm Order.docx

Lieutenant Colonel Mark D. Cyr #2728
Massachusetts State Police
Division Commander
Division of Homeland Security and Preparedness
508-988-7301 (office)
G.L. c. 4.sec. 7.cl.26 (n)(security) *(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: Jason Bianco
To: Hession, Paul (POL)
Subject: Genetec Citigraf overview
Date: Friday, April 7, 2023 9:14:45 AM
Attachments: logocolor(2)_89b44f7c-382f-4530-aee7-d61e3804cc0f.png
emailsignature_ad2b160d-0a28-4983-a2d6-92a7559aa4d9.png
EN-Genetec-Citigraf-Brochure.pdf
Citigraf - 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.

Hi Paul,

I'm not sure if you are aware but wanted to share one of Genetec's products called Citigraf. I attached a general brochure as well as on overview.

In brief summary, it provides a real time crime center integrated to your CAD program as well as GIS and ESRI mapping……and of course being the same platform that you use for video surveillance, license plate recognition, access control, emergency communications and alarm monitoring.

I could coordinate a demonstration if there is any interest on your part.

Thank you.

Jason Bianco
VP, Mission Critical Systems

90 Longwater Drive, Norwell, MA 02061
E: jason.bianco@signetgroup.net
M: (781) 883-6624
signetgroup.net



This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you are not the intended recipient you are notified that disclosing, copying, distributing, or taking any action in reliance on the contents of this information is strictly prohibited. If you have received this email in error, please notify the sender immediately and delete this email from your system.

From: Goddard, Jacquelyn (DOT)
To: Hand, Karissa (GOV); Driscoll, Elaine (EPS); Procopio, David (POL)
Cc: Fennimore, Jillian E. (GOV)
Subject: Hot list questions: reporter deadline is today
Date: Friday, October 20, 2023 3:47:25 PM
Attachments: image001.png
image002.png

Please review this MassDOT comment approved by our law department:

MassDOT draft comment at 3:45 p.m.

- For how long does MassDOT store the license plate data collected at the electronic highway toll booths?

Answer: MassDOT maintains images on its EZPass toll enforcement system for up to 3 years and EZPass toll data for up to 10 years.

- Are vehicles automatically removed from the hot list after 30 days? Are there other methods to make sure they are taken off the hot list in a timely manner or once an emergency ends?

Answer: The Secretary of EOPSS, or their designee, verifies in writing which emergency situations warrant adding any license plate and/or transponder number to the Hot List. License plates and/or transponder numbers only remain on the Hot List for a maximum of 30 days. In most instances, EOPSS will notify MassDOT within hours or just days to cancel the Hot List activation. In the very rare instance when EOPSS does not notify MassDOT within 30 days, MassDOT will notify them that the Hot List activation is being deactivated in accordance with the regulation.

- When a request to add a vehicle to the hot list arrives from State Police or EOPSS, how do MassDOT staff verify that the information is accurate and tied to a permissible use of the hot list?

Answer: License plates and/or transponder numbers are only included on the Hot List in limited 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 sufficient to necessitate the need to provide this Hot List Data to law enforcement. Such emergency situations include terrorist threats, Amber Alerts, Silver Alerts, kidnappings, missing persons, and felons actively traveling to or from a crime scene. EOPSS will state in writing what the emergency situation is that warrants adding a license plate and/or transponder number to the Hot List.

- Our review of email records could not find an instance where MassDOT rejected a hot list request. Are you aware of any instances where that has happened?

Answer: We are not aware of an instance where MassDOT has rejected a Hot List request from EOPSS. EOPSS may have rejected some Hot List requests.

- Has the hot list system been audited before to ensure it is used correctly?

Answer: We are not aware of a MassDOT audit of the Hot List process.

###

DRAFT MSP recommended statement:

MSP Recommended Statement:
"The ability to query information about vehicles connected to serious crimes, through both the MSP's automated license plate readers and the DOT's tolling gantries, is a valuable tool to assist in capturing dangerous offenders, securing justice for their victims, and protecting public safety and homeland security. The MSP utilizes both systems judiciously and in accordance with state and federal laws and Constitutional rights of individuals," –**Mass State Police spokesperson**.

Background:

- Use of the MSP's ALPR system is governed by a rigorous Departmental policy, TRF-11.
- MSP investigators do not have direct access to the DOT gantry information and request such data from the DOT's legal division via a thorough process that ensures all relevant criteria and safeguards are met.

###

From: Hand, Karissa (GOV) <Karissa.Hand@mass.gov>
Sent: Friday, October 20, 2023 10:48 AM
To: Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>; Driscoll, Elaine (EPS) <Elaine.Driscoll@mass.gov>; Procopio, David (POL) <david.procopio@pol.state.ma.us>
Cc: Fennimore, Jillian E. (GOV) <Jillian.E.Fennimore@mass.gov>
Subject: Re: Public Records Request

This is really helpful context, thanks Jacque. Please keep us updated on your responses because we'll want to flag for folks here too.

Karissa Hand (she/her/hers)
Press Secretary
Office of Governor Maura T. Healey

Karissa.Hand@mass.gov
Cell: [redacted]

From: Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>
Sent: Friday, October 20, 2023 10:28 AM
To: Driscoll, Elaine (EPS) <Elaine.Driscoll@mass.gov>; Hand, Karissa (GOV) <Karissa.Hand@mass.gov>; Procopio, David (POL) <david.procopio@pol.state.ma.us>
Cc: Fennimore, Jillian E. (GOV) <Jillian.E.Fennimore@mass.gov>
Subject: RE: Public Records Request

Thanks Elaine. Our highway division and Law Department are currently chasing answers today.

From: Driscoll, Elaine (EPS) <Elaine.Driscoll@mass.gov>
Sent: Friday, October 20, 2023 9:40 AM
To: Hand, Karissa (GOV) <Karissa.Hand@mass.gov>; Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>; Procopio, David (POL) <david.procopio@pol.state.ma.us>
Cc: Fennimore, Jillian E. (GOV) <Jillian.E.Fennimore@mass.gov>
Subject: RE: Public Records Request

Including my most recent inquiry from Will. This is not a topic EOPSS sees regularly, so I need to do more work on my end to get a better handle on the subject matter. As I mentioned, EOPSS did not have any responsive documents to the reporter's PRR request for policies, memos, etc. Dave and I just spoke. Dave recommends providing reporter with MSP's policy on license plate readers (which is specific to MSP's LPRs). He is reviewing whether guidance is included about how to use the DOT's toll gantries. We will work on developing a statement that outlines the rare circumstances when the 'hot list' is used and note it's life-saving capabilities in an emergency and our dedication to balancing public safety and privacy.

From a 2016 Boston Globe story: "The state's new all-electronic tolling system will include a "hot list" feature capable of sending law enforcement officials instant alerts when cars with specified license plates or transponders pass under toll gantries. State transportation officials confirmed the technology is being installed on the Mass."

From Will:
I'd love to chat about the process of using the hot list, how requests are handled, what situations the hot list is most helpful in, and what successes they've had with it.

We'll have a story out this weekend on how the hot list has been used in recent years. If an interview isn't possible today, I would still love to chat with someone and can be available anytime early next week.

If that's the case, I want to make sure EOPSS' perspective is still included in our initial story this

weekend. Would you be able get back to me by the end of today about these questions?

- Has the hot list been a useful public safety tool, and how so? In what cases has the hot list been most helpful?
- Some data privacy advocates voiced concerns about the hot list's use in criminal investigations, since it does not require a warrant to use. How does EOPSS ensure the State Police's requests to add vehicles to the list are accurate and permissible under state regulations?

If you have any other comments you'd like to add, please feel free to include them. Just let me know if I can clarify the questions.

Thanks for your time and help on this.

Best,
Elaine

From: Hand, Karissa (GOV) <Karissa.Hand@mass.gov>
Sent: Friday, October 20, 2023 9:07 AM
To: Driscoll, Elaine (EPS) <Elaine.Driscoll@mass.gov>; Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>; Procopio, David (POL) <david.procopio@pol.state.ma.us>
Cc: Fennimore, Jillian E. (GOV) <Jillian.E.Fennimore@mass.gov>
Subject: Re: Public Records Request

Sorry could someone explain what the hot list is?

Karissa Hand
Press Secretary
Office of Massachusetts Governor Maura T. Healey
Karissa.Hand@mass.gov
Cell: [redacted] G.L. c. 4,sec. 7,cl.26 (n)(security)

From: Driscoll, Elaine (EPS) <Elaine.Driscoll@mass.gov>
Sent: Friday, October 20, 2023 8:59:39 AM
To: Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>; Procopio, David (POL) <david.procopio@pol.state.ma.us>
Cc: Fennimore, Jillian E. (GOV) <Jillian.E.Fennimore@mass.gov>; Hand, Karissa (GOV) <Karissa.Hand@mass.gov>
Subject: RE: Public Records Request

Received. Thanks, Jacque.

From: Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>
Sent: Friday, October 20, 2023 8:56 AM
To: Driscoll, Elaine (EPS) <Elaine.Driscoll@mass.gov>
Cc: Fennimore, Jillian E. (GOV) <Jillian.E.Fennimore@mass.gov>; Hand, Karissa (GOV)

<Karissa.Hand@mass.gov>; Procopio, David (POL) <david.procopio@pol.state.ma.us>
Subject: Fwd: Public Records Request

Elaine,

Good morning.
Please read. I am talking to my colleagues and will be in touch.

Thx
Jacquelyn Goddard
MassDOT Communications Office

Begin forwarded message:

From: Will Katcher <WKatcher@masslive.com>
Date: October 20, 2023 at 8:42:12 AM EDT
To: "Goddard, Jacquelyn (DOT)" <Jacquelyn.Goddard@dot.state.ma.us>
Subject: Re: Public Records Request

CAUTION: This email originated from a sender outside of the 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, Jacque,

We're planning to have a story out this weekend on how the hot list has been used over the past five years. I had a few questions that I wanted to make sure you had the chance to respond to.

1. For how long does MassDOT store the license plate data collected at the electronic highway toll booths?
2. Are vehicles automatically removed from the hot list after 30 days? Are there other methods to make sure they are taken off the hot list in a timely manner or once an emergency ends?
3. When a request to add a vehicle to the hot list arrives from State Police or EOPSS, how do MassDOT staff verify that the information is accurate and tied to a permissible use of the hot list?
4. Our review of email records could not find an instance where MassDOT rejected a hot list request. Are you aware of any instances where that has happened?
5. Has the hot list system been audited before to ensure it is used correctly?

Would you be able to get back to me today? Please feel free to give me a call if I can clarify the questions.

All my best,
Will

Will Katcher
Reporter
MassLive
339-229-1497

From: Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>
Date: Tuesday, October 17, 2023 at 5:37 PM
To: Will Katcher <WKatcher@masslive.com>
Cc: Driscoll, Elaine (EPS) <Elaine.Driscoll@mass.gov>
Subject: RE: Public Records Request

Will,
Good evening.
Re: hot list questions.
I have added Elaine Driscoll to this email as she may be able to provide an interview opportunity on the hot list. Meanwhile, the MassDOT Law Department is still talking to IT in connection with the time frame for records that you still seek.
Thanks,
Jacque

From: Will Katcher <WKatcher@masslive.com>
Sent: Monday, October 16, 2023 3:41 PM
To: Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>
Subject: Re: Public Records Request

CAUTION: This email originated from a sender outside of the 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, I very much appreciate it.

Also, if possible, I would love to chat with someone from MassDOT involved in approving hot list requests. Would a member of the legal team be available to speak this week? I would be happy to keep any conversations on background.

Hope all is well on your end.

Best,
Will

Will Katcher
Reporter
MassLive
339-229-1497

From: Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>
Date: Monday, October 16, 2023 at 3:32 PM
To: Will Katcher <WKatcher@masslive.com>
Subject: RE: Public Records Request

Hi Will – I will circle back with our law department as the lawyer that ran the search that found no records for that time is now out of the office for several weeks. I'll have to ask another attorney to run a search for that time. Thanks

---

From: Will Katcher <WKatcher@masslive.com>
Sent: Monday, October 16, 2023 3:30 PM
To: Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>
Subject: Re: Public Records Request

CAUTION: This email originated from a sender outside of the 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 Jacque,

I appreciate you checking.

When we reported in 2017 on the early uses of the hot list, there were records of at least a half-dozen hot lists requests from that year.

Is it possible these records and others from that time were purged from the MassDOT system, or is there another explanation for why the emails from before Oct. 2018 are no longer available?

Thanks very much for your help.

All my best,
Will

Will Katcher
Reporter
MassLive
339-229-1497
<image003.png>

From: Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>
Date: Monday, October 16, 2023 at 11:28 AM
To: Will Katcher <WKatcher@masslive.com>
Subject: Re: Public Records Request

Will,

Please note regarding you questions in the email below:
The MassDOT Law Department ran a search for MassDOT emails with the date range of 10/28/2016 - 2/22/2023. Based on the search date range, it would appear there were no responsive records prior to October 2018.

###

From: Will Katcher <WKatcher@masslive.com>
Sent: Monday, October 16, 2023 10:23 AM
To: Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>
Subject: Re: Public Records Request (MassDOT) :: P000330-022223

CAUTION: This email originated from a sender outside of the 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 Jacque,

I hope you had a great weekend. I'm just checking back in on this question. Were you able to find whether the additional records exist?

All my best,
Will

Will Katcher
Reporter

MassLive
339-229-1497
<image003.png>

From: Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>
Date: Wednesday, October 11, 2023 at 5:59 PM
To: Will Katcher <WKatcher@masslive.com>
Subject: RE: Public Records Request (MassDOT) :: P000330-022223

I will check, thanks.

From: Will Katcher <WKatcher@masslive.com>
Sent: Wednesday, October 11, 2023 9:50 AM
To: Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>
Subject: FW: Public Records Request (MassDOT) :: P000330-022223

CAUTION: This email originated from a sender outside of the 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 Jacque,

I hope all is well! I'm reaching out regarding the MassDOT Hot List records we received last month. After reviewing the records, it appears the oldest email provided was from Oct. 3, 2018. Our request sought emails dating back to Oct. 28, 2016. Wanted to confirm — does MassDOT not have records prior to Oct. 2018 related to our search?

All my best,
Will

Will Katcher
Reporter
MassLive
339-229-1497
<image003.png>

From: MassDOT Records Center <massachusettsdot@mycusthelp.net>
Date: Wednesday, September 20, 2023 at 3:48 PM
To: CVanBuskirk@masslive.com <CVanBuskirk@masslive.com>

Cc: Will Katcher <WKatcher@masslive.com>
Subject: Public Records Request (MassDOT) :: P000330-022223

Attachments:
attachment_1_Redacted.pdf
Bethel_CT_PD_Silver_Alert1_-_Missing_Person_und_Redacted.pdf
image_Redacted.pdf
image1_Redacted.pdf
Responsive_Records-_P000330_Redacted.pdf
Wanted_Redacted.pdf

--- Please respond above this line ---

September 20, 2023

Will Katcher

Re: Public Records Request for:
"Between Oct. 28, 2016, and Feb. 22, 2023, the number of license plates and/or transponder numbers that have been added to the Massachusetts Department of Transportation's "hot list" as defined in 700 CMR 7.02 and 700 CMR 7.05(8).
The current number of license plates and/or transponder numbers that are on the Massachusetts Department of Transportation's "hot list" as defined in 700 CMR 7.02 and 700 CMR 7.05(8).
Between Oct. 28, 2016, and Feb. 22, 2023, all requests from the Executive Office of Public Safety and Security's Massachusetts State Police "hot list" designee to access hot list data, as defined in 700 CMR 7.05(8), and responses to those requests.
Between Oct. 28, 2016, and Feb. 22, 2023, emails from or to Jamey Tesler, Colleen Ogilvie, Matthew Landry, Michael Ariely, and Erin Deveney containing the following keywords: "Hot list" "Hot list data" "Check toll records" "Host database""

Our Reference No.: P000330-022223

Dear Mr. Katcher,

The records had been sent in August, but I am re-sending as it is my understanding you dod not receive them. The text of our initial response is below:

With regard to "the number of license plates and/or transponder numbers that have been added to the Massachusetts Department of Transportation's 'hot list'", we do not have additional records but the records attached contain all numbers that were added.

With regard to "[t]he current number of license plates and/or transponder numbers that are on the Massachusetts Department of Transportation's 'hot list'", there are zero.

Please be advised that a portion of your public records request seeks information that is exempt from disclosure under Massachusetts General Laws Chapter 4, Section 7(26) (c), which exempts materials or data "relating to a specifically named individual, the disclosure of which may constitute an unwarranted invasion of personal privacy". MassDOT has determined that the public interest in the release of this personal information does not outweigh the privacy interests of the individual(s) involved.

In addition, a portion of the records is exempt pursuant to Massachusetts General Laws Chapter 4, Section 7(26)(a), which is known as the "Statutory Exemption". This exemption provides that records are exempt from disclosure if they are "specifically or by necessary implication exempted from disclosure by statute". In this case, the statute in question is the federal Drivers Privacy Protection Act (18 U.S. Code § 2721) which states, in part, "a State department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity, personal information about any individual obtained by the department in connection with a motor vehicle record...personal information includes the individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information". We cannot, therefore, provide this information as part of a public records request.

In the case of a denial of access to records, you have the right to an administrative appeal to the Supervisor of Records, pursuant to 950 CMR 32.08(1) (the Code of Massachusetts Regulations), and the right to seek judicial review by commencing an action in the Superior Court.

If you need additional information, or there is any other way we can assist you, please respond through the portal or contact our general public records line at (857) 368-8760. Please use our Reference No.: P000330-022223.

Sincerely,

William J. Doyle, Esq.
Records Access Officer
Office of the General Counsel

From: James Sheehan
To: Adam Polhemus; Greg Demeter; Quinn, Dermot (POL)
Subject: I haven't read it yet
Date: Wednesday, February 15, 2023 3:33:33 PM
Attachments: MCCA-Automated-License-Plate-Reader-Technology-in-Law-Enforcement.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.

https://majorcitieschiefs.com/wp-content/uploads/2023/02/MCCA-Automated-License-Plate-Reader-Technology-in-Law-Enforcement.pdf

James J Sheehan
Program Manager
Northern NJ-Jersey City/Newark UASI
30 King Road
Totowa, NJ 07512
(973) 837-7698 Office
[redacted] Cell
Semper et Ubique Fidelis

The information contained in this transmission is for the sole use of the intended recipient(s) and may contain confidential and privileged information and may be considered advisory, consultive and deliberative material under OPRA.
Any unauthorized review; use, disclosure or distribution of this communication is strictly prohibited. If you have received this e-mail in error, please contact the sender by reply e-mail and destroy all paper and electronic copies of the original message

From: Pack, Noah (POL)
To: Cyr, Mark (POL)
Subject: Latest Policy Draft
Date: Monday, March 13, 2023 9:35:13 AM
Attachments: TRF-11 Automatic License Plate Recognition DRAFT 18 3-13-23.docx

---

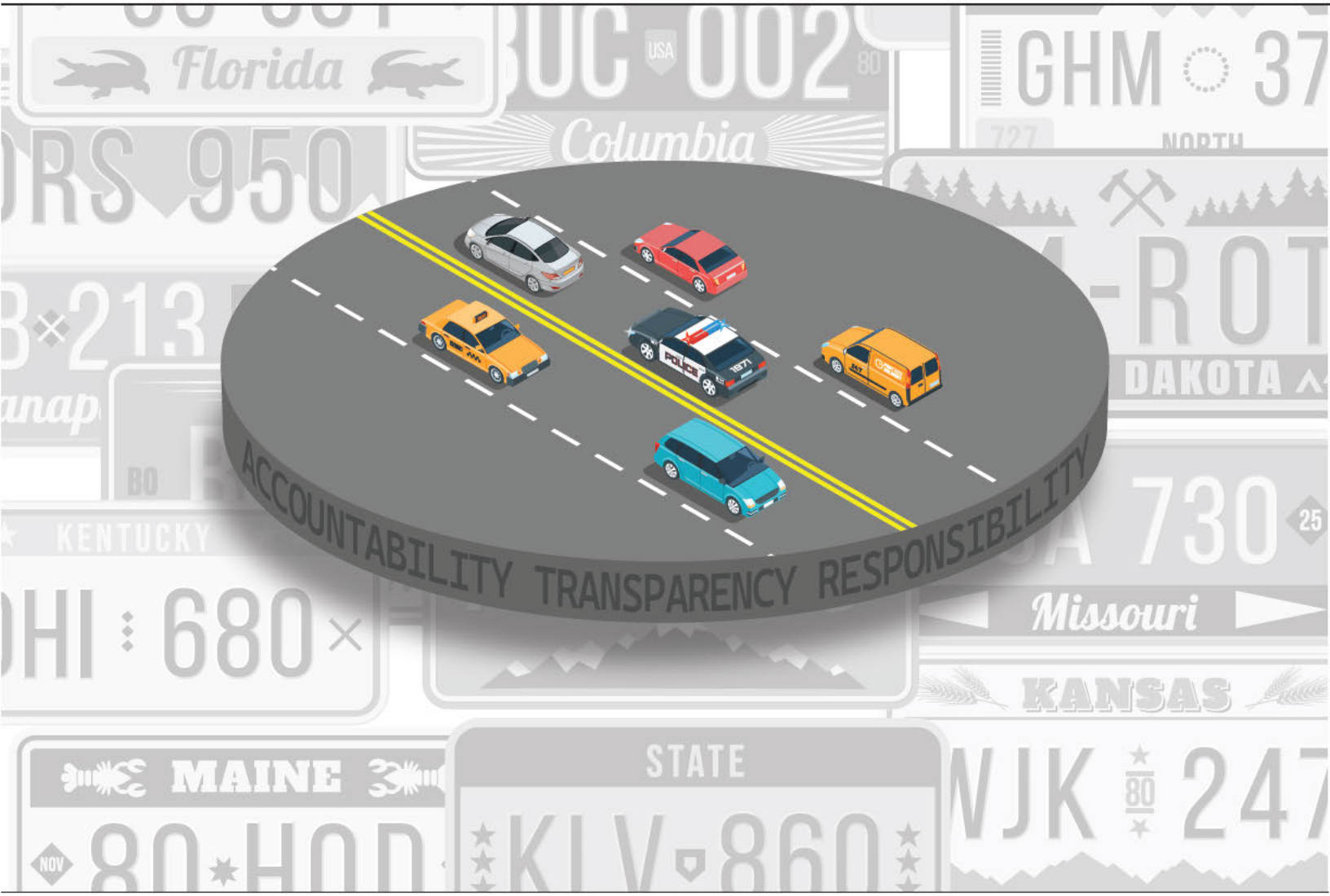
LTC: latest draft attached.

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

MAJOR CITIES CHIEFS ASSOCIATION

Automated License Plate Reader Technology in Law Enforcement

RECOMMENDATIONS AND CONSIDERATIONS



PRESENTED BY MCCA ALPR WORKING GROUP

Table of Contents

Introduction — I
Executive Summary — II
Key Recommendations — III
Methodology of Product — IV
What is an Automated License Plate Reader? — 1
- ALPR Hardware and Software
- Types of ALPR
- The ALPR Detection Record
- Hotlist Sources
- Tactical vs. Investigative Uses
- Business/Private Use

Program Design and Development — 3
- Policy Development
- Training Considerations
- Deployment Strategies

Procurement — 7
- Vendor and Product Assessment
- Technical Challenges
- Procurement Ethics

Program Management and Oversight — 9
- Access and Appropriate Use
- Data Sharing
- Auditing, Data Collection, and Reporting

Data Stewardship — 13
- Data Roles and Responsibilities
- Data Security
- ALPR Reader Device Integrity

ALPR Operations Infographic — 15
ALPR Synergy with Other Law Enforcement Technologies — 16
- Beyond ALPR: AI-Enhanced Vehicle Detection

Case Law Related to ALPR — 17
- Privacy Expectations on Public Roadways
- Is ALPR Persistent Tracking?
- License Plates & Personally Identifiable Information (PII)
- Data Collection & Sharing
- ALPR Hits & Degrees of Intrusion

Conclusion — 21
Acknowledgments — 22
Definitions — 23
Appendix A – Success Stories — 24
Appendix B – Myths and Misconceptions — 26
Appendix C – State-Level Laws and Regulations — 28
Appendix D – CJIS Security Policy — 31
Appendix E – ALPR Audit and Transparency Report Template — 33

1011

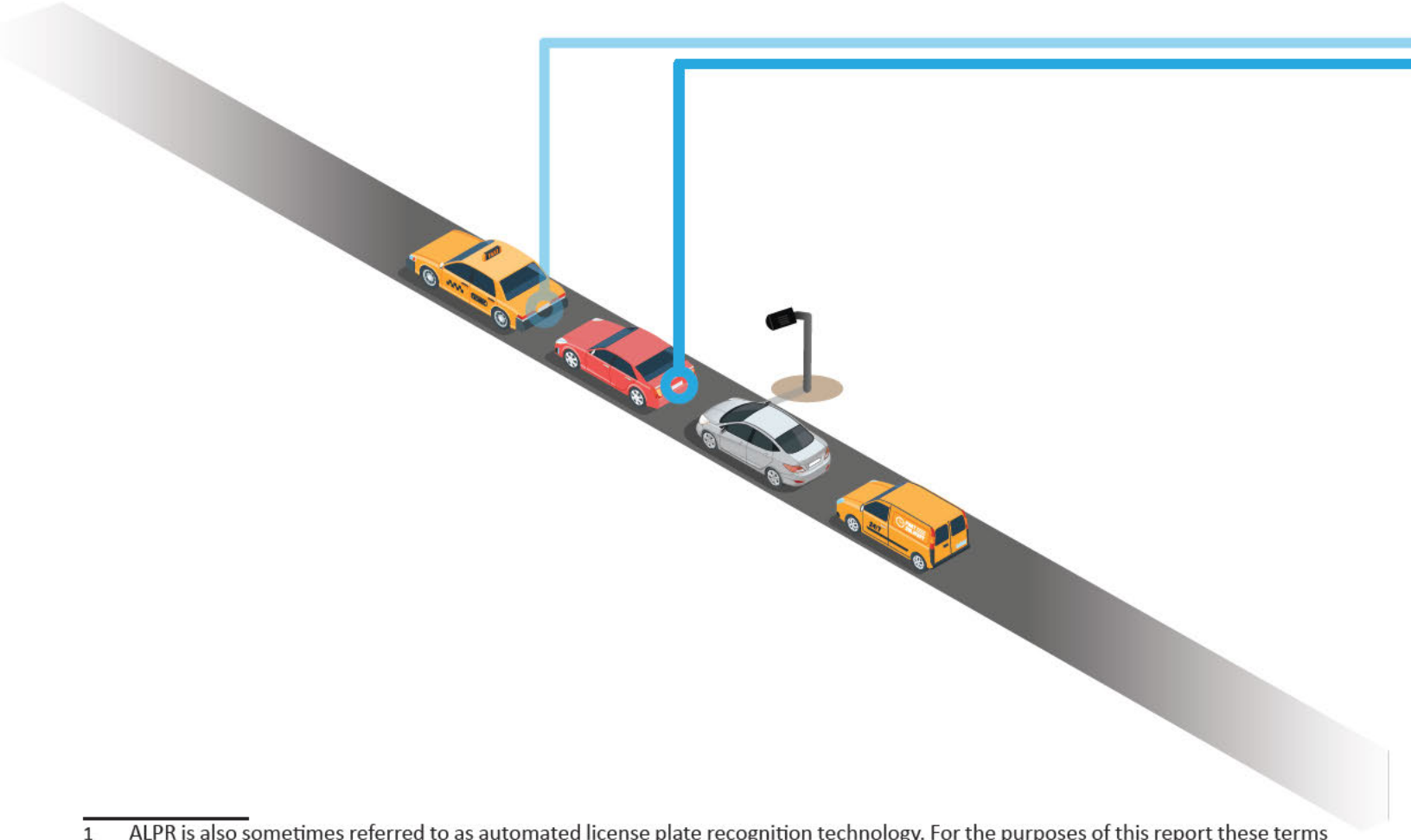
Introduction

Modern-day law enforcement relies on advanced technologies to enhance investigative capabilities. One example of these technologies is automated license plate reader (ALPR).[1] ALPR has been used for decades by law enforcement agencies throughout the United States, Canada, and across the globe to help generate leads and close cases. Law enforcement agencies that utilize ALPR continuously report that the technology is a critical tool that helps advance their efforts to fulfill law enforcement's ultimate mission of keeping our communities safe.

ALPR is a proven technology, but all law enforcement tools must be used ethically and appropriately. This product is designed to assist law enforcement agencies with developing and maintaining an ALPR program that respects citizens' Constitutional rights and privacy while maintaining ALPR's effectiveness as a tool to address crime.

In October 2022, the Major Cities Chiefs Association (MCCA) established an ALPR Working Group composed of trusted technology partners, law enforcement agency stakeholders, and subject matter experts in the ALPR field to achieve this goal. The Working Group has created a set of best practices related to procurement, development, operation, data collection and reporting, and other elements instrumental in creating a well-balanced ALPR program. Like any other technology, ALPR will continue to evolve.

The product is a true public-private partnership, and the framework outlined in it will help law enforcement agencies seeking to utilize ALPR achieve the highest possible standards. However, it is essential to remember that every community is different, and what works in one community may not work in another. Therefore, while the Working Group's recommendations provide a strong foundation, agencies are encouraged to tailor them to meet the specific needs of their community as they develop, implement, and manage their ALPR program.



1 ALPR is also sometimes referred to as automated license plate recognition technology. For the purposes of this report these terms are used interchangeably.

1012

Executive Summary

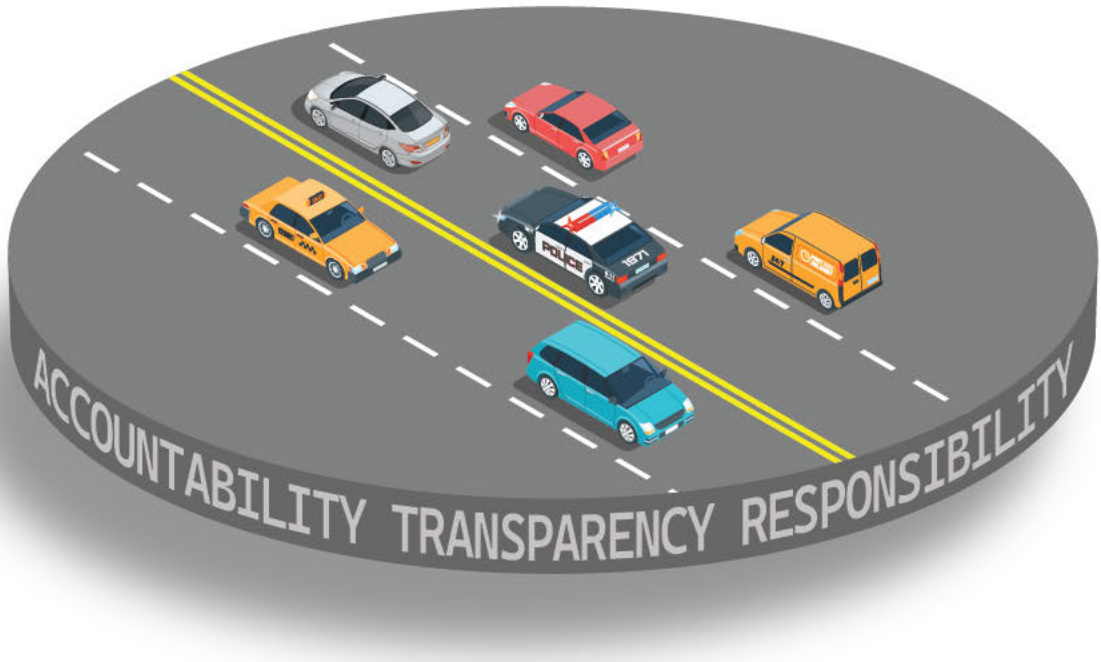
In October 2022, the Major Cities Chiefs Association (MCCA) launched an ALPR Working Group composed of trusted technology partners, law enforcement agency stakeholders, and subject matter experts. The Working Group has developed a product that is designed to provide MCCA members and other law enforcement agencies with guidance on developing, deploying, and responsibly using ALPR technology. ALPR technology has proven to be a powerful tool to combat criminal activity, generate actionable investigative leads, and help close cases faster.

This product directly addresses the most critical aspects of ALPR technology, which can be subdivided into three main categories: accountability, responsbility, and transparency. The product outlines suggestions on ALPR program design, policy development, training considerations, and deployment strategies. The product also covers ALPR procurement. Finally, it addresses the ongoing management and oversight of the technology and provides an overview of relevant case law. While these suggestions and recommendations address the most critical aspects of ALPR, they leave sufficient room for agencies to develop programs that meet their specific needs.

Stakeholders concerned about ALPR typically focus on disparity of impact, infringement of privacy, and the effects on individual rights. However, the Working Group strongly believes these concerns can be sufficiently addressed and mitigated through thoughtful policy design, effective management, and proper oversight. Furthermore, it is important to note that recent case law differentiates the capabilities ALPR provides from those of other law enforcement technologies.

The guidance outlined in this product serves as a template for building and operating an ALPR program that is both effective in its use and responsible in its nature. By implementing the Working Group's suggestions and recommendations, law enforcement agencies can ensure their ALPR programs are helping to keep communities safe while protecting citizens' privacy, civil liberties, and Constitutional rights. In addition, this can help increase public trust and build support for using ALPR technology.

Finally, like all technology, ALPR will continue to change and evolve. For this reason, this product should be considered a living document rather than a finalized template for developing and implementing a balanced and responsible ALPR program. As the conversation surrounding ALPR progresses, so will the recommendations and suggestions included in this product.



1013

Key Recommendations

The following key recommendations serve to highlight the MCCA ALPR Working Group's most essential recommendations and considerations. They have been grouped by their applicability to three foundational principles regarding the deployment of advanced technologies in law enforcement.

ACCOUNTABILITY

- Agencies should develop a training program that establishes accountability guidelines, procedures for responsible use, and emphasizes transparency. The use of ALPR technology should be limited to trained personnel.
- The use of ALPR technology should be limited to criminal investigations or to address an articulable public safety concern.
- The procedures for the use of ALPR technology should emphasize the need to confirm the accuracy of the information presented prior to taking enforcement action.
- Careful consideration should be given to the data retention policies implemented by the agency. Data retention time frames should be developed by balancing community needs, benefits, and concerns.
- Audits of ALPR programs should be conducted regularly. Audits should monitor user activity to ensure appropriate use in accordance with established policies.

RESPONSIBILITY

- Sharing ALPR data among law enforcement agencies can enhance the effectiveness of ALPR deployments. A clear policy should be established prior to enabling data sharing to address data usage and deconfliction requirements.
- Deployment strategies should be reviewed regularly and evaluated to ensure the ALPR program and technology continues to operate within the established objectives and policies.
- Law enforcement agencies seeking to procure ALPR technology should consult with other agencies that have deployed ALPR during program development.
- Prior to the deployment of ALPR technology, agencies should assess existing technological deployments and consider how they can complement or enhance their specific program strategy.
- Law enforcement agencies must implement strict cybersecurity protections to prevent unauthorized access of ALPR data.

TRANSPARENCY

- Deployment plans should be informed by analyzing crime data, patterns, and trends to ensure the technology is deployed in an equitable and responsible manner.
- Agencies should consult with their local public works and other relevant stakeholders to ensure the ALPR deployment plan meets all permitting, legal, and other requirements.
- Comprehensive data collection and reporting will help maximize the benefits of ALPR technology by increasing transparency and empowering agencies to determine its impact on crime and public safety.

Methodology of Product

This product represents the comprehensive collection of the MCCA ALPR Working Group's recommendations and considerations regarding law enforcement's use of ALPR technology. The value of ALPR as a crime-fighting tool is well established. However, an effective program must include certain elements to ensure the technology is being used effectively and in a manner that maintains the trust and support of the community. This document will provide law enforcement agencies with a framework to develop, implement, and manage an ALPR program that is based on responsible use, helps keep the community safe, and respects privacy, civil rights, and civil liberties.

The MCCA ALPR Working Group includes technology vendors from various backgrounds, a diverse group of law enforcement professionals, and ALPR subject matter experts. In addition, the Working Group conducted in-depth research on ALPR technology from numerous perspectives. Finally, the Working Group leveraged the expertise of the individual participants to develop its recommendations and suggested best practices.

The information and data used to support the findings of this product include material provided by MCCA member agencies and technology vendors. The Working Group also reviewed products produced by other stakeholders on ALPR and the use of technology in policing more generally. Finally, the Working Group conducted regular internal discussions to finalize the recommendations and suggested best practices.

This product's outline and overarching topics were created collaboratively with input from all Working Group participants. Each participant was responsible for drafting a section of the report, and those drafts were circulated to the entire Working Group for review. All Working Group members approved the final product.

The final product represents the MCCA ALPR Working Group's findings, recommendations, and suggested best practices. These will help law enforcement agencies create, manage, and operate an effective and responsible ALPR program.

What is an Automated License Plate Reader?

ALPR, called Automated Number Plate Recognition (ANPR) in Europe, was invented in 1976 by the Police Scientific Development Branch to combat terrorism in the United Kingdom. While seen as a valuable tool, the associated cost and requisite experience stagnated the deployment and advancement of the technology until the first ALPR cameras were installed at the Dartford Tunnel and A1 Road in 1981. The Dartford Tunnel cameras resulted in ALPR's first arrest for a stolen vehicle. This slowly led to more widespread use of the technology, including as part of the "ring of steel" created around London in the early 1990s to protect against the Irish Republican Army (IRA) bombing campaigns. Later, ALPR technology was also deployed as part of another initiative entitled "Project Laser," which sought to "target criminals through their use of roads."[1]

The success of the "ring of steel" and "Project Laser" prompted the Police Standards Unit to create the National ANPR Data Centre (NADC) in 1997. The NADC allowed for the nationwide sharing of ALPR data across the United Kingdom and the Back Office Facility (BOF), the database where ALPR data was stored and analyzed. ALPR technology took off from here. Law enforcement first used ALPR to help solve a murder case in 2005, and by 2007, nearly half of all law enforcement agencies in the UK were using ALPR technology. American law enforcement agencies followed their British counterparts closely and started using ALPR in 1998.[2]

ALPR Hardware and Software

While the technology has advanced over the years, the main components of those early ALPR deployments and today's systems remain the same. At its core, an ALPR program consists of the camera hardware and the software used to store and analyze the generated data and alert the users when a detection of interest is made. In most cases, ALPR hardware consists of a camera, processor, power supply, and data transfer hardware. In addition, ALPR cameras are typically optimized in various ways to operate in a wide range of real-world conditions (low light, inclement weather, motion detection, etc.).

Once the camera captures the image, ALPR systems use software to read the license plate. Some systems process the image at the camera level. Other systems transfer (usually via a cellular network, but it may occur through other means) data from the camera to a dedicated ALPR-system computer for processing. The image is analyzed through Optical Character Recognition (OCR) software as part of the processing. OCR recognizes alpha-numeric numbers and letters, thereby allowing the ALPR system to successfully recognize and interpret any letters or numbers observed in the image captured by the camera.

Types of ALPR

Law enforcement uses various types of ALPR technology, including fixed, mobile, portable, and mobile applications. Below is a description of each kind of ALPR system:

- **Fixed ALPR** cameras are typically permanently mounted to infrastructure such as traffic signals, bridges, and light poles.
- **Mobile ALPR** cameras are typically mounted on vehicles. These cameras may be overtly or covertly deployed depending on the needs of the law enforcement agency.
- **Portable ALPR** cameras include mobile camera trailers which can be transported and deployed based on the law enforcement agency's operational needs.
- **Mobile Applications** leverage features built into cellular devices to create ALPR detections.

1 David J. Roberts and Meghann Casanova, Automated License Plate Recognition (ALPR) Systems: Policy and Operational Guidance for Law Enforcement, National Institute of Justice, U.S. Department of Justice, 2012. https://www.ojp.gov/pdffiles1/nij/grants/239605.pdf

2 B.A. Reaves, Local police departments, 2013: Equipment and Technology. Bureau of Justice Statistics, U.S. Department of Justice, July 2015. https://bjs.ojp.gov/library/publications/local-police-departments-2013-equipment-and-technology

The ALPR Detection Record

An ALPR record is generated when a vehicle license plate is detected, imaged, and processed to create a record. An individual ALPR record (or 'plate read') is generally composed of the following:

- An image of the license plate, which is a 'cropped' digital image of the license plate captured by the camera.
- The geo-location where the plate detection occurred, which can be determined from the GPS coordinates of a mobile reader or inferred from the location where fixed readers are placed.
- The time and date when the license plate detection occurred.
- The translated information from the plate, which is the alpha-numeric plate number and the issuing organization, typically a state. This translation can be accomplished by OCR or artificial intelligence.

In addition, an ALPR record may contain the following:

- A collateral image of the vehicle for which the ALPR read occurred.
- Metadata associated with the camera that identifies the camera unit, image settings, and other specific attributes.

Hotlist Sources

ALPR systems used by law enforcement can alert on detections of wanted vehicles. Two primary methods exist for creating a wanted vehicle within an ALPR system. First, ALPR systems allow for the manual entry of both a hotplate and a hotlist. Second, the ALPR system allows agencies to import National Crime Information Center (NCIC) records as an automated hotplate source. This is the most common method for populating hotlists.

Tactical vs. Investigative Uses

Law enforcement typically uses ALPR technology for both tactical and investigative purposes. Accordingly, agencies should consider both uses when developing their ALPR program's objectives. A tactical ALPR deployment includes placing cameras in strategically identified locations to generate information that warrants a rapid police response, such as stopping a wanted vehicle. These deployments usually seek to identify, locate, and recover a vehicle or its occupants to help address crime occurring in real time. An investigative use refers to utilizing ALPR cameras to collect license plate records that may have law enforcement interest but do not necessarily warrant an immediate police response. These detections are stored in the system and may later be queried. This information is generally used to create an investigative lead after a crime has occurred.

Business/Private Use

Since ALPR systems provide valuable data, private businesses and other organizations have also invested in ALPR technology. These uses may be for security, management, or operational needs. The following are examples of private sector use cases:

- Parking garages
- Hotels and casinos
- Homeowners associations
- Airports
- Convention centers
- Government traffic and transportation sites



Program Design and Development

ALPR has proven to be a successful law enforcement tool. Its unique ability to provide actionable leads and help close cases cannot be overstated. However, real and perceived concerns exist regarding this technology's use. Therefore, law enforcement must take careful steps to develop an ALPR program that is both effective and appropriate. Taking a thoughtful approach when designing and developing these programs is the best strategy to accomplish these goals. Some of these considerations include developing proper policies, creating comprehensive training material, and designing and implementing responsible deployment strategies.

Policy Development

Establishing clearly defined policies on how ALPR may be used is the most effective method to minimize risk to the agency and protect both department employees and the individual rights of the public. ALPR policy should direct the purpose, general use, and processes involving ALPR investigations. These policies will provide a framework by which an agency can simultaneously reap the benefits of the technology, all while respecting the privacy and civil rights of the public. Similarly, consistent policies will assist in protecting the integrity of criminal investigations, criminal intelligence collection, and justice system processes. The following components should be considered while developing ALPR policies and procedures:

- Community-directed statement on why the agency is establishing or maintaining an ALPR capability
- The purpose of the policy
- General use guidelines of the technology
- Clearly defined program oversight roles and responsibilities
- The ALPR vendor and deployment types
- Access, training, and usage requirements
- Investigative procedure requirements
- Clear guidance to department employees on being transparent on the use and reporting of the technology in court documents
- Auditing responsibilities and schedule
- Data retention and purging
- Statement affirming protections for constitutionally protected activities
- Rules governing the use of hotplates

State/Local Law Considerations

Many state legislatures have taken steps to regulate the use of ALPR technology in their states. These laws and regulations can directly impact the functioning of an ALPR program in those states, and they must be accounted for in agency policy. Examples of the types of rules and regulations implemented in several states can be found in Appendix C – State-Level Laws and Regulations.

Training Considerations

Ensuring a thorough training program is in place is critical. Users must receive training on the ALPR system before receiving access. This practice ensures ALPR systems are only used for official law enforcement purposes consistent with applicable legal limitations and department policy. The training program should address several topics to ensure that users of an ALPR system are proficient in the necessary skills, including:

- A review of the departmental policy and safeguards related to ALPR use
- Basic understanding of how the technology operates
- The ALPR data sources, vendor, type of systems, etc.
- Any significant capabilities and or limitations related to the technology
- Any potential hazards related to the technology

1018

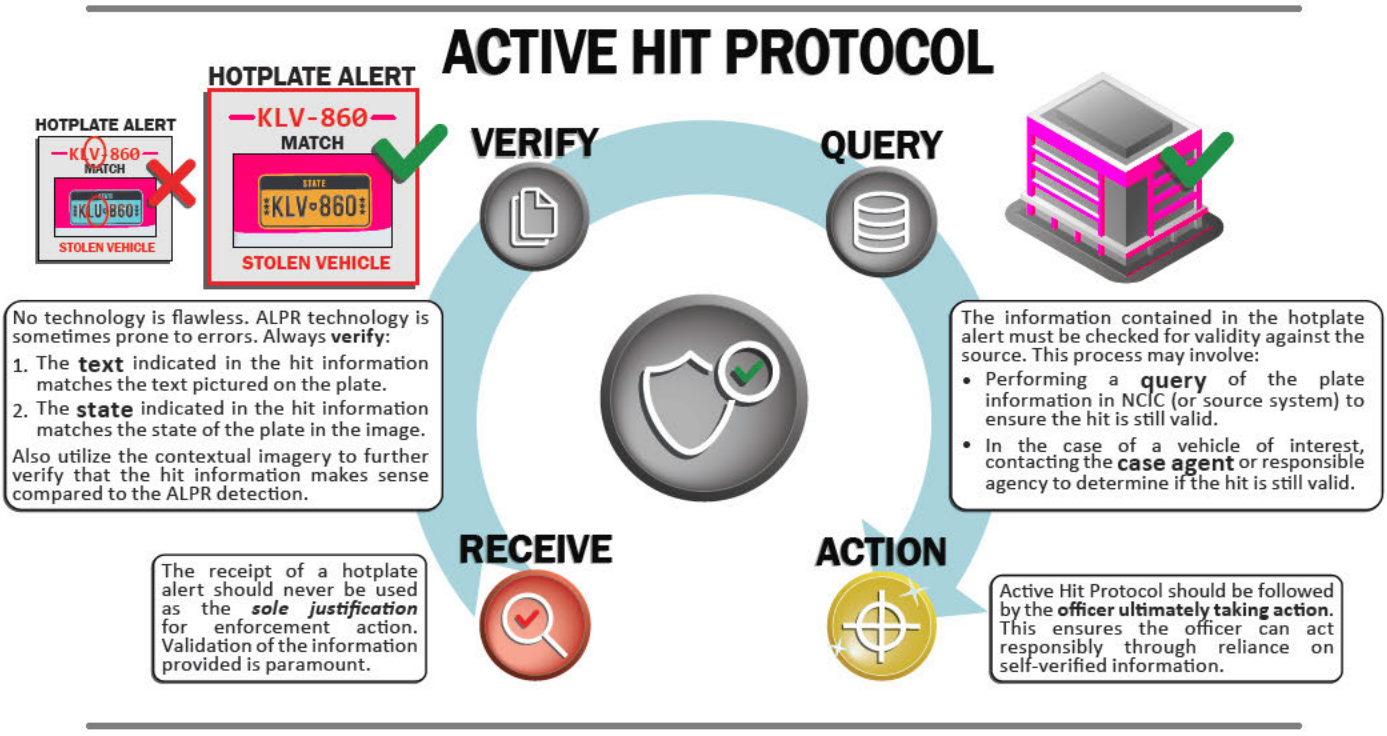
- Who is authorized to access the system and any required training
- The role of the officer or investigator in leveraging and responding to ALPR hotplate detections
- Importance of being transparent with arresting documentation
- Any applicable laws and policies that govern the use of ALPR in the specific jurisdiction
- Use of the ALPR system as an investigative tool
- The data retention period
- Auditing responsibilities

An ALPR training program should include a tactical-level discussion of how to use the technology appropriately. For mobile units, this should consist of an initial check to ensure that the ALPR system is operating correctly at the beginning of each shift. This includes logging into the system, running any necessary diagnostics to determine that it is working correctly, and doing a quick physical inspection of the system (cameras, cables, connections). In addition, a program manager should conduct periodic checks of fixed ALPR sites to verify that the hardware is operational and communicating with the software as intended.

Field Officer Responsibilities

A critical piece of the officer training on ALPR should include an element that instructs how ALPR notifications are processed and the appropriate response protocols for those notifications. Some departments may have fixed ALPR hits reviewed and confirmed by the public safety answering point or real-time crime center before dispatching them to an officer to investigate. Other systems may provide an in-car alert on the car computer system.

Officers should be required to review hotplate detection, confirm the detections, and appropriately respond to actively wanted vehicles. This process can be referred to as "Active Hit Protocol."



Investigator Responsibilities

The ALPR system is a valuable investigative tool. It can be used to develop leads in cases involving vehicles where the license plate is unknown or to establish that a car was not in the vicinity during the time frame a crime occurred. An ALPR training program must include how to access the system and the criteria required before conducting a query, such as the reason for the search and the associated case number. Additionally, investigative tool training should address how to query the system, instructions on operating the various analytical tools within the system, how to interpret the data, how to preserve a record, and any required transparency, audit, or reporting requirements.

Types of Training

Training should be broken down into multiple categories:

- **New User Training:** This training will be detailed and define proper usage. In addition, this training should include policy, procedures, state and local laws, and an in-depth walk-through of the ALPR products and software.
- **Refresher Training:** This is considered a refresher of policy and procedures. It may also include changes to case law and examples of ALPR use. This training should ideally occur immediately after any changes to policy take place.

Authorized instructors should provide training on ALPR technology based on an established, accredited curriculum. An example of an accredited curriculum is one that has been approved by the state's Peace Officer's Standards and Training (POST) or equivalent body.

Deployment Strategies

Determining the ALPR deployment type and kind is one of the most critical decisions an agency will make concerning its ALPR program. Law enforcement is responsible for deploying advanced technology in a manner that is effective in its use and appropriate in its scope. Law enforcement also has a fiduciary duty to use public funds responsibly. For these reasons, ample consideration should be made when determining the type and kind of ALPR deployment.

ALPR Deployment Theories

As previously addressed, various types of ALPR technology exist, including fixed, mobile, portable, and smartphone applications, with each serving a unique purpose. Therefore, the kind of ALPR selected should be determined by the environment, infrastructure, and objectives for the ALPR deployment. Several ALPR deployment strategies are often considered when determining the value and placement of ALPR cameras. The most common of these strategies include the following:

- **High Traffic Areas:** The primary objective is to collect the maximum number of detections that can later be leveraged for investigative leads.
- **High Crime Areas:** This strategy focuses on producing information anticipated to be of investigative value instead of creating as many detections as possible.
- **Places of Interest:** This strategy is more of a hybrid between the first two. An example of this strategy would be deploying ALPR cameras around a shopping mall targeted by organized retail theft gangs or where assaults have occurred. Agencies may also place ALPR cameras in proximity to their community's major ingress/egress points and critical infrastructure or routes associated with gun, drug, or human trafficking.

1020

Deployment Considerations

Infrastructure and permitting are two common factors that can limit an agency's deployment strategy for ALPR systems. Agencies must carefully consider each physical deployment site. The infrastructure to mount the necessary hardware must exist for the technology to be successfully deployed. Furthermore, the owner and operator of the infrastructure or property must allow for the installation of ALPR hardware. Agencies must also ensure that the proposed site is appropriate for the type of power the ALPR utilizes. Some systems run on AC power. While this provides constant and consistent power, installing it can be more expensive. Others rely on solar energy, which may only provide enough power if the camera site receives sufficient sunlight to account for the traffic volume. Finally, this infrastructure must have access to a data transmission service, such as cellular, fiber optic, or Wi-Fi.

Once a deployment plan has been established, site locations have been determined, and in-person inspections of the sites have been completed, the agency will need to navigate any legal and permitting processes. Since permitting can vary significantly across jurisdictions, it is recommended that agencies consult with their local public works or other appropriate governmental entities to ensure all necessary procedures are being met. Engaging these entities earlier in the process will help secure their buy-in, which will be critical for a successful deployment.

Equitability Concerns

Deployment strategies must account for concerns over bias, surveillance or other threats to privacy, and potential chilling effects on First Amendment, defendant, or related rights. The following recommendations will help ensure ALPR technology is deployed in a manner that supports just and equitable policing:

- Deployment plans should be informed by analyzing crime data, patterns, and trends. The site selection process should be based on this information and account for any relevant privacy, equitability, or other concerns.
- Agencies should consult the community, other stakeholders, and appropriate oversight committees. This includes providing specific information on why and how the deployment sites were selected.
- Deployment strategies should regularly be reviewed and evaluated to ensure the ALPR program and technology continue s to operate within the established guidelines and policies.

Partner Technologies

While developing the deployment plan, it is important to consider other law enforcement technologies that may complement the ALPR system. Law enforcement agencies may deploy complementary technologies within the same area, which have different capabilities. Agencies can leverage these capabilities to increase their ability to suppress crime, create actionable leads, solve cases, and potentially deter future crimes. Potential partner technologies can be subdivided into two categories: tactical and investigative.

Tactical technologies include tools such as gunshot detection technology, public safety cameras, and drone detection technology. An example of investigative technology is a records management system (RMS). Integrating ALPR and RMS can join plate reads to hotlists, allow investigators to search plate reads within a familiar interface, and provide a direct link between case management and the ALPR database. Another example of investigative technology is crime analysis software. Bringing ALPR data into an agency's chosen analysis software can aid in ongoing investigations. For example, agencies can import ALPR data to help create accurate timelines for vehicle travel that can provide investigators with unseen leads and valuable knowledge.

1021

Procurement

Responsible procurement of ALPR technology is a critical component of an effective program. The importance of obtaining stakeholder feedback early in the procurement process cannot be understated. Program managers should make every effort to embrace a spirit of transparency, accept critical feedback, and attempt to address any concerns raised by stakeholders directly.

The procurement phase is also the appropriate time to begin building departmental policies, procedures, and protocols, as this will be crucial in gaining stakeholder buy-in. It is imperative that the stakeholders understand how these policies will protect the public's privacy and civil liberties. Agencies should also seek to mitigate any concerns that stakeholders raise about the proposed ALPR program through thoughtful policy design.

Vendor and Product Assessment

Before choosing a vendor for their ALPR program, law enforcement agencies should conduct an appropriate degree of market research. This should include a trial of the product and conversations with existing customers to evaluate its performance in a real-world setting. A trial period provides the opportunity to test the technology, the associated policies and procedures, and highlight initial successes. This can provide tangible examples that can be shared with stakeholders to show how ALPR serves to enhance public safety.

Should an agency engage in a pilot program, it is recommended that the community be notified. Agencies should also determine how any information collected may be used in investigations or other law enforcement operations until a final protocol and all other areas of the program are formalized.

When determining the best hardware for their ALPR program, law enforcement agencies should consider the following:

- Hardware requirements for specific sites
- The lenses, processor, and other technical specifications of the hardware
- Average detections per hour
- General cost
- The number of lanes of traffic a single camera can capture
- The maximum speed at which the camera can read a license plate

When determining the best software for their ALPR program, law enforcement agencies should consider the following:

- The accuracy of the OCR software and whether it's enhanced by artificial intelligence, machine learning, or another capability
- The technology's alerting system, including desktop, laptop, mobile, app-based, and in-car alerts
- The software's ability to connect and share data with other law enforcement analytical platforms

Technical Challenges

There are some challenges with ALPR software that agencies must acknowledge. For example, OCR technology analyzes all letter or number sequences in the imagery; it cannot specifically isolate only license plate images. Therefore, a detection can be created on something that is not a license plate. This includes billboards, signage, marketing material on vehicles, etc. Additionally, the full license plate letter and number sequence must be visible to create an accurate license plate detection. Occlusion, missing plates, and temporary paper plates may result in no detection, a partial detection, or a misread.

Misreads may occur for several reasons, but most are due to the incorrect translation of a letter or number. For example, the system may read an "8" as a "B" or a "K" as an "X." These technical challenges should be readily acknowledged by both the agency and a prospective ALPR vendor. Agencies must ensure their policies account for these challenges and contain sufficient safeguards to limit instances where officers act based on a misread or other error.

1022

Procurement Ethics

While local procurement ordinances vary across jurisdictions, agencies must follow those ordinances along with broader guiding principles when procuring an ALPR platform. The National Institute of Governmental Purchasing's (NIGP) Values and Guiding Principles of Public Procurement are one such set of broad principles that agencies can use to inform any ALPR procurement process. The NIGP principles are as follows:

- **Accountability:** Taking ownership and being responsible to all stakeholders for our actions. This value is essential to preserve public trust and protect the public interest.
- **Ethics:** Doing the right thing. This value is essential to deserve the public's trust.
- **Impartiality:** Unbiased decision-making and actions. This value is essential to ensure fairness for the public good.
- **Professionalism:** Upholding high standards of job performance and ethical behavior. This value is essential to balance diverse public interests.
- **Service:** Obligation to assist stakeholders. This value is essential to support the public good.
- **Transparency:** Easily accessible and understandable policies and processes. This value is essential to demonstrate the responsible use of public funds.[3]

3 Additional information on NIGP's Guiding Principles can be found here: https://www.nigp.org/our-profession/values-and-guiding-principles-of-public-procurement

Program Management and Oversight

An ALPR program's design and operational management are part of the framework of a successful program. Effective management and oversight of the program help ensure operational transparency and accountability and that ALPR technology is being used responsibly.

To ensure the program operates responsibly, agencies should assign a manager operational control of the ALPR program. This individual should be well versed in the technology, have a sound understanding of all significant components of the ALPR program, and be empowered to ensure the program follows protocols, policy, applicable law, and community and agency expectations.

A program manager's responsibilities include the following:

- Developing policies
- Overseeing training
- Ensuring appropriate use of the technology
- Managing data collection and reporting

A program manager is also responsible for staying current on technology changes and emerging ALPR trends. Similarly, they must ensure that their agency's ALPR policies and training are current and address technological changes or advancements. Finally, having a program manager establishes a clear point of contact between the law enforcement agency and the ALPR vendor. This can enhance the communication between the agency and vendor, which creates an opportunity to share and address any technological or other challenges.

Access and Appropriate Use

Law enforcement agencies are responsible for using ALPR data to uphold public safety, solve crimes, and prevent future crimes. Agencies have an opportunity to build public trust and support for the use of ALPR through transparency and responsible use. As such, agencies should carefully consider the circumstances under which using ALPR is appropriate and what personnel within the agency can access this tool.

Law enforcement agencies must scope their ALPR programs in a manner that ensures the agency is still able to conduct proper oversight and operate the program transparently. One method for achieving this is by limiting who can access the ALPR technology. For example, many law enforcement agencies restrict access to specialized personnel to ensure that the use of ALPR technology is adequately audited and controlled. Access should only be authorized once a user has completed the requisite training and demonstrates a baseline understanding and operational knowledge of the technology. Information on new user training, access, and use should be part of standard data collection and reporting related to the ALPR program.

Agencies that deploy ALPR must have written policies that outline the appropriate use of the technology. Several core principles should be incorporated into these policies to ensure the responsible use of the technology. First and foremost, ALPR technology should only be used as part of a criminal investigation or to address an articulable public safety concern. Secondly, the investigator must also have a legitimate "need to know" before querying any ALPR data. These guardrails will help prevent "curiosity checks" or other bad faith uses and ensure that privacy, civil rights, and civil liberties are respected.

Agency users must also demonstrate adherence to established policies when searching archived ALPR data. For example, if the ALPR software allows it, agency policy should require users to document the investigative purpose and case number associated with each query. Vague or ambiguous reasons for a search, such as "criminal subject" or "research," should be avoided. An agency's ALPR policies should also outline the potential consequences and corrective methods for improper use of the technology. Examples may include mandatory retraining, loss of access privileges, or other appropriate corrective punishments.

1024

Data Retention

Data retention policies are ultimately determined by the agency using ALPR technology. These policies are informed by various considerations, including the agency's objectives, stakeholders' expectations, and local laws or regulations. Therefore, it is essential that the ALPR technology, vendor, and any other relevant service providers support the agency's policies on retention.

While a general best practice is not to retain data any longer than is necessary, what constitutes "no longer than necessary" is not a simple determination since different use cases may benefit from different retention periods. For example, cold cases may benefit from years-old data, while other uses rely on more recent data.

Outside of specified legal requirements, the retention schedule for ALPR data is primarily determined by agency policy.[4] As such, law enforcement must work with the community and other stakeholders to determine appropriate retention periods for each type of ALPR data. Ideally, ALPR systems should allow agencies to define retention schedules and automatically purge any record not designated for retention by a registered user. In addition, regular system audits ensure retention standards are followed and instill confidence that system data is utilized appropriately.

Data Sharing

For good reason, law enforcement agencies worldwide are embracing ALPR technology. A 2013 Bureau of Justice Statistics study showed that 77% of agencies serving populations of 100,000 or more have access to ALPR technology.[5] Moreover, given ALPR technology's value to a single jurisdiction, law enforcement has begun to explore sharing ALPR data across jurisdictional boundaries. Sharing ALPR data amongst law enforcement agencies fosters a more collaborative approach to addressing public safety concerns across jurisdictional boundaries.

Benefits of Data Sharing

When law enforcement agencies share ALPR data across jurisdictions, the technology can provide more comprehensive data. A shared system creates more unified and robust coverage throughout a region. Several ALPR vendors currently provide their law enforcement customer base with the ability to share data with other law enforcement customers. The potential to cross-reference information between separate ALPR systems allows law enforcement to enhance their investigative capabilities and can reveal elements of illegal activity that may otherwise be unknown to the investigating agency. Several elements of ALPR data and systems can be shared, including the ALPR detections and user-created hotlists. Some ALPR vendors also allow agencies to establish data-sharing relationships between their products and other technology systems.

As a standard practice, law enforcement agencies should consider sharing ALPR data with one another to the extent that state or local laws and regulations permit. Agency policy should define what, if any, type of data sharing is in place, who is authorized to establish data-sharing relationships, and any procedures that govern the sharing of ALPR data. These procedures and data-handling agreements should be implemented in policy for both the sharing and receiving agencies.

The success of ALPR technology among law enforcement has led non-government entities to acquire the same technology. This includes retailers, property managers, towing and repossession companies, parking lot operators, homeowner associations (HOAs), and even individual households. Since the generated data is of the same format and often targets issues of mutual interest, ALPR vendors have created Public-Private Partnership (PPP) friendly user interfaces. These programs typically allow the unidirectional sharing of ALPR data from the non-government side to the law enforcement side only. These partnerships strengthen community relationships and ensure public investments are used responsibly.

4 David J. Roberts and Meghann Casanova, Automated License Plate Recognition (ALPR) Systems: Policy and Operational Guidance for Law Enforcement, National Institute of Justice, U.S. Department of Justice, 2012. https://www.ojp.gov/pdffiles1/nij/grants/239605.pdf

5 B.A. Reaves, Local police departments, 2013: Equipment and Technology. Bureau of Justice Statistics, U.S. Department of Justice, July 2015. https://bjs.ojp.gov/library/publications/local-police-departments-2013-equipment-and-technology

1025

Data Sharing Considerations

While data sharing benefits agencies, safeguards are needed to protect the agency that generates and owns the data. Data sharing guidelines can be specific to the type of shared data. For instance, if agency "A" shares ALPR detection data with agency "B," there may be no requirement for a formal agreement. In contrast, if agency "A" shares hotplates or agency-generated hotlists with agency "B," this scenario may require a formal agreement. This is because hotplates or hotlists are typically generated from a criminal investigation or law enforcement process or function that may require an officer to take action if there is a confirmed detection. Furthermore, the agency that receives the information should bear the responsibility and liability for their officers' actions in response to an alert.

Law enforcement agencies seeking to share or receive ALPR data must be aware of applicable federal, state, and local laws. As such, agencies should consult with their legal representatives to identify pending, proposed, or existing laws that may be relevant. For example, legislation is proposed annually at all levels of government which, if enacted, could limit law enforcement data sharing. Finally, agencies must consider any concerns from the community or other stakeholders before establishing multi-jurisdictional data-sharing relationships.

Auditing, Data Collection, and Reporting

Auditing and reporting an agency's use of ALPR technology is a critical component of a transparent and accountable ALPR program. The failure to operate a program in this manner will only exacerbate concerns related to misuse or contribute to the perception that ALPR technology is synonymous with increased surveillance. This will undoubtedly negatively impact police-community relations. Agencies should develop robust mechanisms to evaluate the efficacy of the technology and ensure it is being used appropriately.

Auditing Requirements

Regular audits on an ALPR system are one method for validating compliance with agency policies and applicable laws and regulations. As with other reporting requirements, the specific auditing measures, and the frequency of said audits, should be clearly defined in the ALPR program's governance documents. In general, audits should verify what ALPR information was accessed and by whom, in order to identify any improper or unauthorized uses of this data. Audits should also ensure that data within the system is being handled per agency policy, including information sharing agreements. They should also confirm that data is being purged as required under any applicable data retention schedules.

Data Collection and Reporting Considerations

Studies have shown that ALPR technology is most effective when used systematically and when deployment sites are strategically selected.[6] In addition, comprehensive data collection and reporting will assist agencies with maximizing the benefits of ALPR technology. Finally, robust data collection and reporting will help increase transparency.

At a minimum, agencies using ALPR should collect and report the following information:

- Number of detections
- Number of hotplate hits
- Number of queries conducted by users
- Number of arrests directly attributed to ALPR hotplate detections
- Number of user-generated hotplates
- Breakdown of hotplate hit types
- Year-over-year analysis and trends

By analyzing this data, agency leaders and stakeholders can determine whether their ALPR system is meeting deployment goals and has significantly impacted crime or other areas of police operations. ALPR data collection and reporting also provide valuable insight into ALPR system adoption throughout the organization.

6 C. S. Koper and C. Lum, "The impacts of large-scale license plate reader deployment on criminal investigations," Police Quarterly, 22(3), 305–329, 2019. https://doi.org/10.1177/1098611119828039

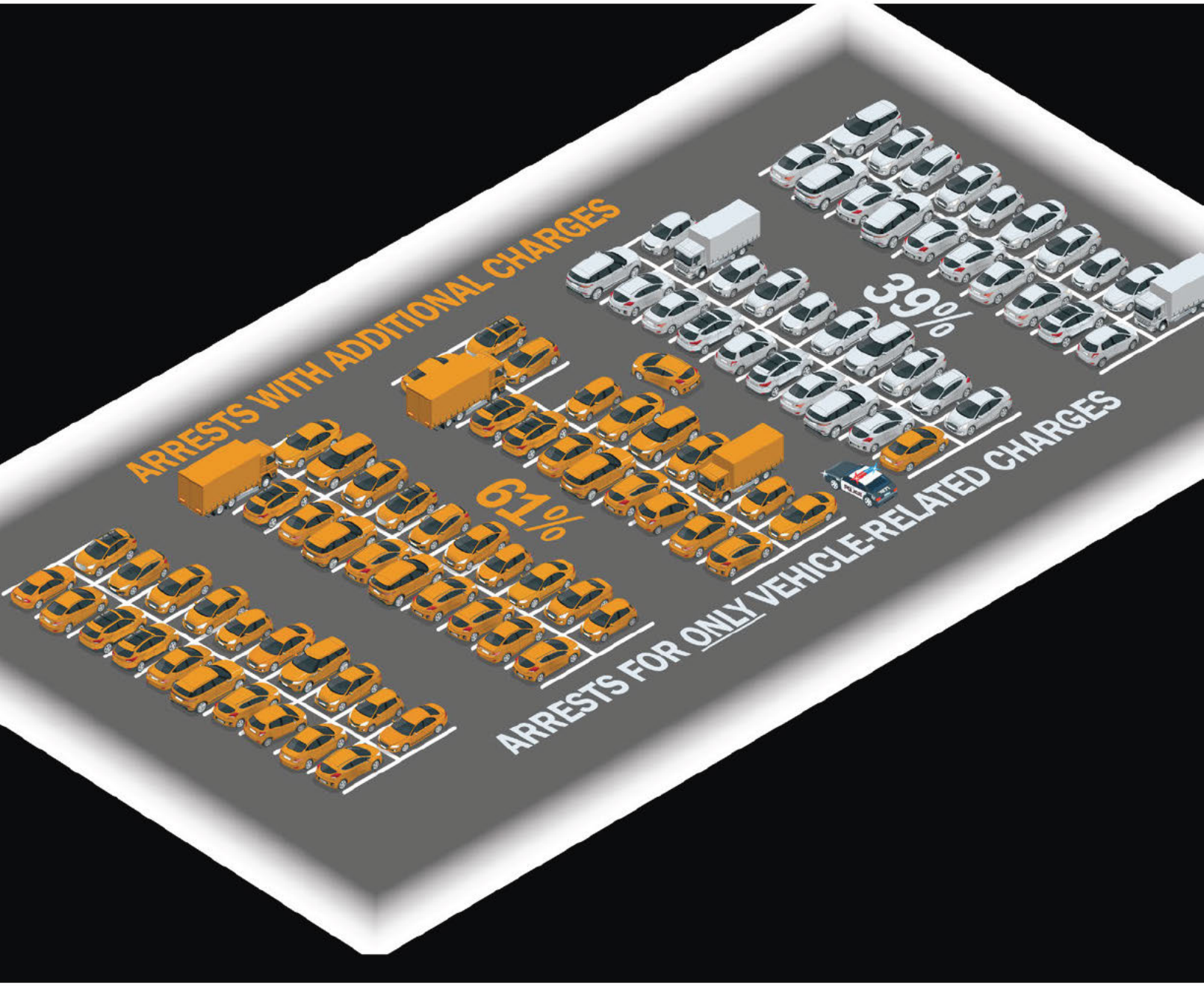
1026

The Importance of Analysis and Reporting

Quantitative data is an excellent tool to measure the impact of law enforcement technology. The ability to answer the questions "how many" and "how often" is necessary to evaluate real-world outcomes. Additionally, the quantitative analysis of ALPR data can provide an agency and stakeholders with the information needed to determine the impact of the technology on community safety.

To explore the potential of quantitative reporting, an MCCA member agency recently analyzed the impact of a localized ALPR deployment. The data presented below represents a period of four months after the installation of ALPR cameras within the evaluated area. The types of charges related to any arrests resulting from an ALPR event were analyzed. The data suggests that ALPR technology generates leads and solves more types of crimes than those related to ALPR's most frequent use: the recovery of stolen vehicles.

It is important to capture and analyze the impact of any ALPR program to dispel misconceptions and demonstrate the impact of the technology.



1027

Data Stewardship

Throughout the design of an ALPR program, the hardware, software, and policies implemented will shape how ALPR data is collected and stored. Therefore, a comprehensive strategy should be developed to ensure all data collection aspects are secured and managed effectively.

Data Roles and Responsibilities

ALPR records are typically stored in databases that can be indexed, searched by individual or composite conditions, and analytically processed by applications that power ALPR use cases. This is an important and powerful compilation of data that must be managed judiciously. The two primary roles relative to this data are data owners and service providers.

The data owner is the organization that controls the data and decision-making authority. The data owner, typically the data's generator and user, determines how the data may be used, who it can be shared with, and its retention limits. For example, law enforcement is always the data owner for the ALPR data it generates. While this data may be shared with other law enforcement entities, the owner and provider of any particular data always retains control over all aspects of it. Therefore, other organizations that have received access to that data must act in accordance with the data owner's direction, such as adhering to retention limits established by the owner on the data.

A service provider is an entity that may take possession of data to store or process it on behalf of the data owner. The service provider operates at the behest of the data owner and enacts the owner's wishes and directions. This can include management of data sharing with other designated users, enforcing retention limits, etc. The service provider has no entitlement to the data and may not sell, derive secondary insights, or otherwise share it. Furthermore, they may only access the data to perform a function at the direction of the data owner. Law enforcement agencies often hire an outside company to be their service provider for ALPR data.

Storing and Processing ALPR Data

There are several general models for storing and processing ALPR data:

- The data is stored on-premises and processed by applications under the direct physical control of the organization that generates and uses the data.
- The data is stored off-premises by a cloud service provider and processed by applications in the cloud or on-premises under the direct control of the organization that generates and uses the data.
- The data is stored in the cloud or at an off site data center and is processed by a service provider.

In the first model, the data owner is effectively their own service provider, and there isn't necessarily a third party service-providing entity. The other two models imply some degree of a third party service provider. In those cases, the data may be held or accessed by another entity on behalf of the data owner. For ALPR systems, this could be either a cloud computing service or an ALPR technology vendor. However, in both cases, control of the data remains with the data owner.

Data Security

Law enforcement agencies should treat ALPR data like any other sensitive data it collects, uses, and manages. It should be protected as judiciously as law enforcement records, video, and other critical operational data. This includes ensuring responsible usage of the data by law enforcement personnel and vetting any service providers that may process the data. Law enforcement agencies must also apply rigorous cybersecurity practices to protect and secure the ALPR data it generates and uses. This includes, but is not limited to, proper authentication methods (multi-factor authentication is generally considered a best practice), data-sharing controls, and role-based access controls for users. Law enforcement agencies must ensure that their technology vendors provide adequate security practices to protect the ALPR data they possess and process on behalf of the agency.

Whether a service provider provides on-premise technology, stores data on behalf of a law enforcement agency, or hosts the processing applications, they have an important role in ensuring the secure and trustworthy operation of an ALPR program. The service provider is responsible for securing the data it processes to protect it from unauthorized access, theft, or misuse. They must provide the necessary capabilities, controls, and training to enable law enforcement agencies to enforce their own defined data governance policies, security standards, and procedures. This includes:

- **Enforcement of Retention Limits:** This may be applied absolutely or in a role-based fashion. For example, the absolute retention limit for ALPR data could be three years, but only cold case investigators may access data older than six months.
- **Positive Controls Over How Data is Shared:** Data must only be shared after law enforcement specifically enables it with individual partners at its discretion and under the auspices of its policies.
- **Enforcement of Personnel Controls:** These controls include system and user-level authorization, role-based access controls, and regular audits.

The FBI's Criminal Justice Information Services (CJIS) Security Policy provides a comprehensive reference and standard that agencies may use to design or measure data management for their program. For cases where service providers take possession of ALPR data from law enforcement agencies to store and process on their behalf, agencies should consider using the CJIS Security Policy to assess and set expectations of service providers.[7] An explanation of relevant sections of the CJIS Security Policy can be found in Appendix D – CJIS Security Policy.

As mentioned earlier, cloud services may be part of an agency's ALPR program. These services' security and integrity depend on the efficacy of the underlying cloud platform. Cloud service providers (or service providers that operate their own data center directly) should comply with ISO 9001:2015, an internationally recognized standard for Quality Management Systems. Compliance with this standard should be independently audited and verified for compliance under the Statement of Auditing Standards Number 70 [SOC 2 Report]. In addition, compliance with FedRAMP medium security controls provides an additional level of validation and may be required for information sharing with federal entities. Even though license plate detection records are not personally identifiable, they may be linked through other sources that may enable the end user to input data that could be viewed as personally identifiable or criminal justice information.

ALPR Reader Device Integrity

An ALPR reader that captures ALPR images and does local image processing contains instances of ALPR data. This data may be transient or stored on the device for extended periods. Since ALPR readers are often distributed in the environment and may be difficult to physically secure, it is increasingly important to consider the device's ability to locally secure ALPR data that is either at rest or in motion. FIPS (Federal Information Processing Standards) 140 standards are used to evaluate the hardware and software integrity of cryptographic modules. This applies to many devices, including ALPR readers, that need to encrypt data to secure it from compromise. FIPS 140-2 is broken into four, successively increasing levels of security.[8]

- FIPS 140-2 Level 1 is the lowest and imposes limited requirements.
- FIPS 140-2 Level 2 adds requirements for physical tamper-evidence and role-based authentication.
- FIPS 140-2 Level 3 adds requirements for physical tamper-resistance (making it difficult for attackers to gain access to the sensitive information contained in the module) and identity-based authentication, and for a physical or logical separation between the interfaces by which "critical security parameters" enter and leave the module, and its other interfaces.
- FIPS 140-2 Level 4 makes the physical security requirements more stringent and requires robustness against environmental attacks.

Depending upon the specific environment where it is deployed, the ALPR reading device should, at a minimum, support FIPS 140-2 Level 2. Aspects of FIPS 140-2 Level 3 are also becoming increasingly desirable and necessary, especially as ALPR technology advances.

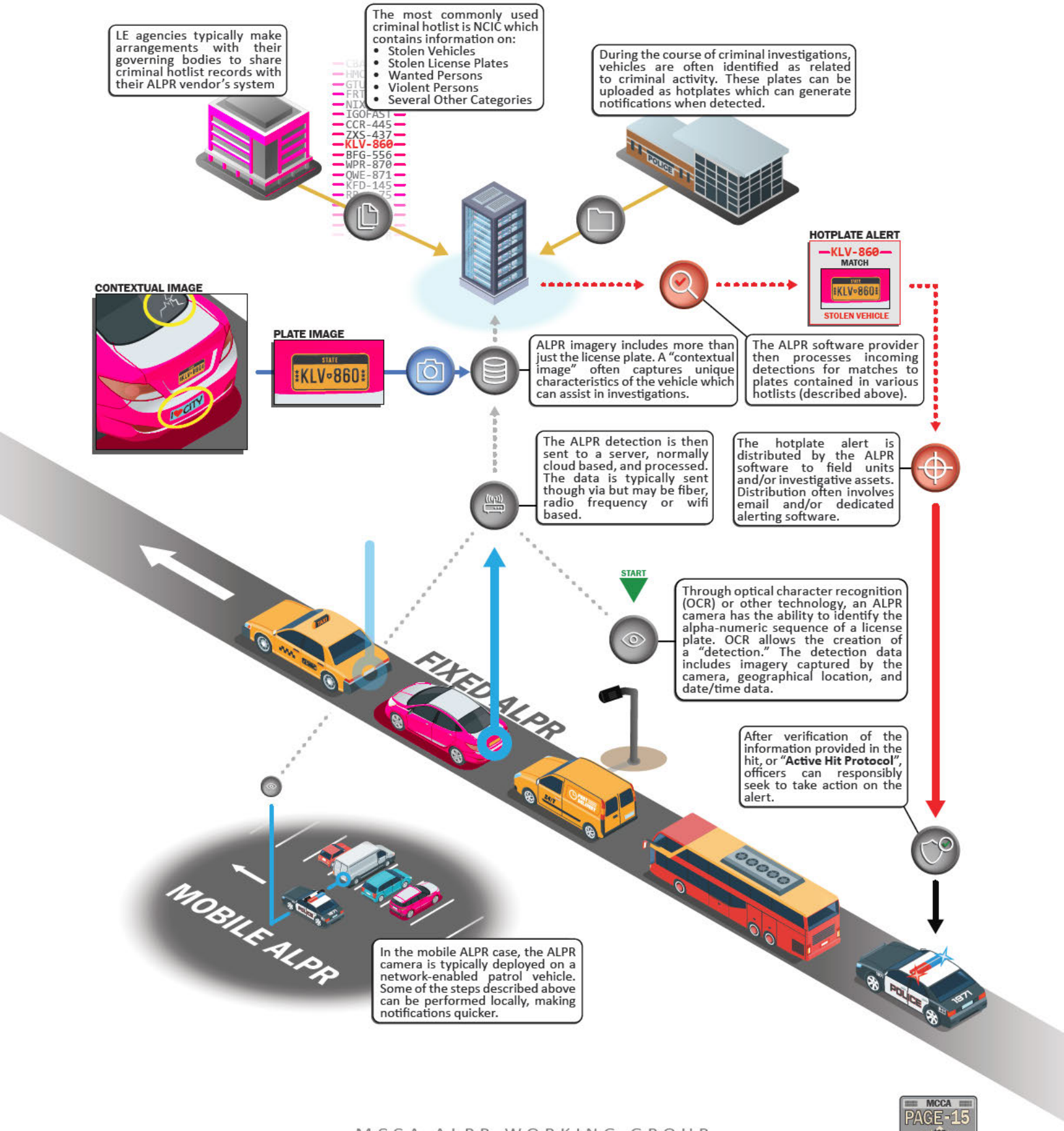
7 Criminal Justice Information Services (CJIS) Security Policy, CJISD-ITS-DOC-08140-5.9.1, US Department of Justice - Federal Bureau of Investigation, Version 5.9.1, October 22, 2022.

8 A. Lee, M. Smid, S. Snouffer, Security Requirements for Cryptographic Modules [includes Change Notices as of 12/3/2002], (NIST FIPS), National Institute of Standards and Technology, 2001. https://doi.org/10.6028/NIST.FIPS.140-2

1029

ALPR Operations Infographic

Several aspects of the operation of ALPR technology can be better understood when put in the context of the technological workflow.



1030

ALPR Synergy with Other Law Enforcement Technologies

As law enforcement gains access to more information, technology will help ensure the data is organized so law enforcement officers can solve complex policing problems. Any single data source, such as ALPR, only answers one of many questions. It only tells law enforcement where a vehicle was at a given time. ALPR alone does not answer critical questions such as whom the car belongs to or who has been associated with it before, whether any of those individuals have a history of involvement in similar incidents, and other critical questions.

By integrating data across common law enforcement data sources, those questions can be asked and answered immediately, drastically increasing the odds of solving cases. Here are a few examples:

> *Consider a situation where CCTV footage captures a partial plate on a vehicle shortly after the commission of a crime. In an ideal scenario, an ALPR database may be queried to determine the rest of the characters on the license plate. Then a separate RMS system could be queried to determine if that license plate has ever been mentioned in a case report.*
>
> *A platform has ALPR, RMS, citation, and crash data integrated into one place. An ALPR detection can be searched and then linked to see if that plate has been named in an RMS case, vehicle citation, or crash report, along with any involved individuals. Links between vehicles, people, and incidents can be seen without having to search each database individually.*
>
> *An ALPR alert occurs in a platform that has CAD & CCTV integrated. As a result, an immediate CAD call can be created to accompany the alert, and any relevant CCTV footage in the area can be attached and sent to the responding officer, better preparing them to engage with the vehicle that triggered the alert.*

In these examples, a singular piece of information would have failed to fully identify the suspect vehicle. It is the utilization of an ALPR database in conjunction with other technologies produces an actionable investigative lead. For ALPR detections to be used to their fullest potential, that data must be connected to other relevant data sets.

The ultimate goal of connected data should be to allow for insights that are impossible to see currently or take too much time to consider. Departments should own all their data, including ALPR detections, and be able to link, connect, or integrate data sets as department leadership deems appropriate. When developing an ALPR program, agencies should ensure their vendors are aligned with this perspective and are capable of facilitating integrations with other law enforcement technology.

Beyond ALPR: AI-Enhanced Vehicle Detection

With advances in image processing technology, specifically those afforded by artificial intelligence and machine learning, it is becoming increasingly possible to identify a vehicle solely from an image. Artificial intelligence is able to focus on characteristics of a vehicle such as make, model, color, or distinguishing attributes/markings. These advanced image processing technologies improve the accuracy of ALPR systems and allow law enforcement to corroborate ALPR information. For example, they could assist with confirming that the vehicle associated with a detection matches the description in the registration record. Image-based detection and identification will continue to advance and improve the efficacy of ALPR technology.

Case Law Related to ALPR

License plates are required in every state to display proof of registration. Registration identifies a particular vehicle and confirms that it meets minimum state-mandated safety requirements to be operated on public roadways. In addition, operators of vehicles must be licensed to drive legally on public roads.

It is possible in many states to own a vehicle and, if it is never parked or operated on a public roadway, not be required to display license plates. Furthermore, one can own a car but have no authority to operate it, just as one can be licensed to drive a car but never actually own one. Collecting information related to people and vehicles are separate and distinct concepts, although not entirely mutually exclusive. The alpha-numeric characters of a license plate alone do not indicate who owns the vehicle or is licensed to operate it.

For more than 50 years, the United States Supreme Court, and many lower courts, have repeatedly acknowledged that vehicles are inherently subject to greater regulation when operated on public roadways. In the age of enhanced technology, ALPR invokes specific legal considerations:

- Reasonable privacy expectations of those in vehicles on public roadways
- Persistent tracking and the nature of ALPR technology
- The nexus between license plates and personally identifiable information
- Collecting and sharing ALPR data
- The degree of intrusion authorized by an ALPR hotplate detection

An examination of existing case law related to these concepts follows. There is often no bright-line precedent when considering emergent technology. In such instances, reasonable legal conclusions can be inferred from cases related to other technology and privacy issues already adjudicated by the courts.

Privacy Expectations on Public Roadways

In 1967, the U.S. Supreme Court clarified in *Katz v. U.S. (1967)* that "the Fourth Amendment protects people, not places." [9] The Fourth Amendment of the United States Constitution ensures:

> *[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.*

In *Cady v. Dombrowski (1973),* the U.S. Supreme Court noted that vehicles, while "effects," are constitutionally different from a person's home. The case also referenced the regularity with which police engage in activity unrelated to the enforcement of laws, such as maintaining the efficiency of the flow of traffic and ensuring the safety of those using the roadways. The Court acknowledged that this regular contact with automobiles contributes to police being more often in "plain view" of evidence, instrumentalities of a crime, or contraband.[10]

Delaware v. Prouse (1979) offers historic guidance concerning the constitutionality of stopping or seizing vehicles. The U.S. Supreme Court cites, "the permissibility of a particular law enforcement practice is judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests."[11] One can reasonably infer that photographing a plainly visible license plate, on a public roadway, or from a location plainly visible from a lawfully authorized location, with no intrusion upon the vehicle occupants or otherwise interfering with their movement or affecting any person's possessory interest in the vehicle or license plate, is not a seizure constitutionally.

Lower courts have routinely ruled that law enforcement officers may, without specific suspicion, check the status of a license plate against a law enforcement database.[12][13] Therefore, searching aggregated photographs, which contain no specific information about a particular vehicle owner or operator, even when correlated with additional information such as the time, date, and location of the photograph, does not constitute a search.

9 Katz v. United States, 389 United States Supreme Court. 347, (1967). https://supreme.justia.com/cases/federal/us/389/347

10 Cady v. Dombrowski, 413 United States Supreme Court. 433 (1973). https://supreme.justia.com/cases/federal/us/413/433

11 Delaware v. Prouse, 440 United States Supreme Court. 648 (1979). https://supreme.justia.com/cases/federal/us/413/433

12 Jones v. Town of Woodworth, Court of Appeal of Louisiana. 15-568. (2015). https://caselaw.findlaw.com/la-court-of-appeal/1717448.html

13 State v. Davis, 237 Or. App. 351, 239 P.3d 1002, Oregon Court of Appeals. (2010). https://caselaw.findlaw.com/la-court-of-appeal/1717448.html

Is ALPR Persistent Tracking?

The notion that vehicle travel on public roadways is an unavoidable element of modern living merits consideration, given how ALPR is deployed. Recent U.S. Supreme Court rulings related to law enforcement's use of other technologies have considered the inescapable and automatic nature of data collection. An analysis of these rulings is offered to differentiate the substantially greater capabilities of such technologies compared to those of ALPR.

Two recent U.S. Supreme Court rulings merit particular consideration for the use of technology to investigate the historical movement of persons. In *U.S. v. Jones (2012)*, the U.S Supreme Court held that police need a search warrant to install a covert GPS tracking device on a vehicle to monitor its location for an extended period of time. In *Carpenter v. U.S. (2018),* The Court ruled that police must secure a warrant before obtaining cell-site location information from service providers regarding an individual's location history.

The theme of both cases concerns the capacity that modern technology affords the government to explore comprehensive, specifically personal location information, which was not possible until the advent of recent ubiquitous technology. GPS and cell-site location information enable persistent automated tracking of a targeted individual's activity with such detail and scope that the techniques constitute a search. In the case of *Carpenter v. U.S. (2018),* the Government obtained 12,898 location points cataloging Carpenter's movements. This extensive amount of information amounted to an average of 101 data points per day during the period they obtained historical records.[14]

An ALPR system cannot independently predict life patterns accurately or be used to conduct real-time surveillance of any person or vehicle. Even if police acted with willful disregard for the protections of the Fourth Amendment, it is impossible to accomplish such a degree of ongoing surveillance using ALPR technology. A fixed ALPR camera may be able to collect information about every car that passes its location. Still, the data is limited to an otherwise anonymous characteristic of the vehicle, not automatically attributable to any individual without accessing other restricted databases, and for only a single moment in time at a single location.

Images of plates stored in the ALPR database are retained and made available for specified queries. Tangential information may include the nature of a vehicle's location, direction of travel, and any criminal justice information associated with the detection. As to the question of whether a collection of images from multiple cameras, aggregated in a searchable database implicates Fourth Amendment considerations, the US Supreme Court has not taken up precisely to what extent ALPR coverage, or how robust an ALPR database is, may trigger specific Fourth Amendment implications.

In *Commonwealth v. McCarthy (2020)*, the Massachusetts Supreme Judicial Court concluded that "While the defendant has a constitutionally protected expectation of privacy in the whole of his public movements, an interest which potentially could be implicated by the widespread use of ALPRs, that interest was not invaded by the limited extent and use of ALPR data in this case." The case involved law enforcement's use of four ALPR devices on two bridges to investigate a defendant's movements during a period of two months. In that case, the court ruled that the limited use of ALPR data did not violate the defendant's reasonable expectation of privacy.[15]

License Plates & Personally Identifiable Information (PII)

Individuals (people) are licensed, but a vehicle is registered. A vehicle is registered with an organization (typically a state), which then authorizes the vehicle to be driven on public roads and highways by a licensed driver. For example, passenger and commercial vehicles must be registered as a condition of use on a public thoroughfare. Upon registration, the state department of motor vehicles then issues a license plate which must be attached to the vehicle and openly displayed for vehicle identification purposes. The purpose of a license plate is to identify a vehicle uniquely, and it does not include personally identifiable information of any individual. By itself, a license plate number is an anonymous code unless combined with other registration information containing owner/operator information (i.e., a department of motor vehicles database or an employee or homeowner registration). Thus, an ALPR record is generated from publicly available data and corresponds with detecting a vehicle, not an individual, at a specific location and time.

The federal *Driver's Privacy Protection Act (DPPA)* was enacted in 1994 to "protect the personal privacy and safety

14 Carpenter v. United States, United States Supreme Court. 585 (2018). https://supreme.justia.com/cases/federal/us/585/16-402

15 Commonwealth v. McCarthy, 484 Massachusetts Supreme Judicial Court (2020). https://cases.justia.com/massachusetts/supreme-court/2020-sjc-12750.pdf

1033

of licensed drivers consistent with the legitimate needs of business and government." DPPA made it "unlawful" to access, disseminate, or otherwise misuse information held by a state's motor vehicle office, including information related to both drivers and vehicles, without the owner's consent or for another legitimate, legally authorized purpose, such as criminal justice purposes. ALPR systems do not automatically link to data governed by DPPA. Law enforcement can only obtain such protected information from other secure, access-restricted criminal justice databases.

The case of *Harrison Neal v. Fairfax County Police (2020)* examined the use of an ALPR system to passively scan and retain license plates that were not on a hotlist to determine if such a practice violated the state's *Government Data Collection and Dissemination Practices Act.*

A key element of the case was whether an ALPR system constitutes an information system governed by the Code of Virginia. The court found that the ALPR system did not, noting that the ALPR database can be searched only by license plate number, not by any person's information. Furthermore, the system does not gather identifying information about the vehicle owner. To acquire such personal data, an officer must query a wholly separate criminal justice database via a different computer program.[16]

California Code 1798.29 specifically expands the meaning of "personal information" to include information or data collected through the use or operation of an ALPR system. While not adjudicated by any court, ALPR information is considered personal information in California due to unique state legislation.

Data Collection & Sharing

A license plate is a required government instrument specifically intended to identify the vehicle to which it is affixed publicly. In the case of *United States v. Ellison (2006)*, the Court noted:

> *This court has yet to address in a published opinion the question of whether an individual has a reasonable expectation of privacy regarding their license plate. In two unpublished decisions, however, this court has agreed with the other circuits that have decided this issue by holding that no such privacy interest exists. The reasoning of these opinions, as well as that of the Supreme Court in related cases, leads us to agree that a motorist has no reasonable expectation of privacy in the information contained on his license plate under the Fourth Amendment.*[17]

Publicly viewing or photographing a displayed license plate constitutes activity protected by the First Amendment of the United States. The cataloging and subsequent sharing of such data remain largely regulated by state or local legislation. In the case of *U.S. v. Yang (2020),* the Ninth Circuit ruled that the defendant did not have standing to challenge government queries of a vendor's ALPR database for records of his movement when he kept a rental car beyond the contract due date. The court noted that Yang failed to establish that he had a reasonable expectation of privacy in the historical location information of the vehicle that was the subject of the query. The Court declined to address any potential privacy interests related to the warrantless use of ALPR technology.[18]

16 Harrison Neal v. Fairfax County Police, Record No. 191127, Supreme Court of Virginia (2020). https://cases.justia.com/virginia/supreme-court/2020-191127.pdf

17 United States v. Ellison, 462 F.3d 557, 561, United States Supreme Court. (6th Cir. 2006). https://caselaw.findlaw.com/la-court-of-appeal/1717448.html

18 United States v. Yang, No. 18-10341, United States Court of Appeals for the 9th Circuit (2020) https://law.justia.com/cases/federal/appellate-courts/ca9/18-10341/18-10341-2020-05-04.html

ALPR Hits & Degrees of Intrusion

Several cases have affirmed that an ALPR hotplate detection, also referred to as a "hit," constitutes sufficient reasonable suspicion to affect a traffic stop. For example, in the case of *Hernandez-Lopez v. State (2013)*, the Georgia Court of Appeals held that an ALPR system merely aided the officer by augmenting his sensory faculties and that based on the alert provided by the ALPR, the officer had reasonable, articulable suspicion to conduct a traffic stop. [19]

Similarly, in the case of *Traft v. Commonwealth (2018)*, the Supreme Court of Kentucky held that an officer obtaining information linked to his license plate did not violate the defendant's rights under the Fourth Amendment. This information indicated that Traft had an outstanding bench warrant and, therefore, reasonable suspicion existed to stop the vehicle. Furthermore, the court noted that the license plate "was displayed in a place where he had no reasonable expectation of privacy."[20]

In the case of *Green v. City and County of San Francisco (2014)*, an ALPR system returned a hit based on a misread. The officer was transporting a prisoner at the time and could not verify the hit's validity. The image on the ALPR was "dark and blurry." The officer subsequently provided a description of the vehicle via police radio, including the incorrect license plate indicated by the ALPR system, not the actual plate displayed on the car. Dispatch ran the plate as provided and noted that it belonged on a pick-up truck.[21]

A second officer observed Green's sedan bearing the plate as broadcast by the first officer. However, this officer also failed to confirm whether the radioed license plate number matched the plates on Green's car. Consequently, Green was stopped, challenged at gunpoint by multiple officers, placed on the ground, and handcuffed. Green filed suit against the defendants, alleging claims under 42 U.S.C. 1983 and California state law for wrongful detention, false arrest, and excessive force. The Ninth Circuit ruled that "an unconfirmed hit on the ALPR does not, alone, form the reasonable suspicion necessary to support an investigatory detention."

While legally permissible to affect a stop based on an ALPR hit, independent verification of the validity of an ALPR alert should be considered a best practice. Verifying that the actual vehicle license plate and the read on the ALPR screen are safeguards against a potential unjustified intrusion upon any person. Such guidance should neither cause officers to hesitate when officer safety is a concern nor preclude officers from acting on indicators amounting to reasonable suspicion based on other observations coupled with their training and experience. However, inappropriate outcomes resulting from the use of law enforcement technology can have substantial repercussions on perceptions of police legitimacy and the continued availability of such tools.

In conclusion, ALPR systems detect license plates in public locations collecting information that is generally not considered private. Critical elements of an ALPR system, such as the extent of camera coverage, reasons for selecting fixed deployment locations, length of time that data is retained, and the extent to which the information is shared, may factor in with respect to if an ALPR system implicates Fourth Amendment considerations. The consistently responsible use and thoughtful deployment of ALPR technology will ensure that all civil rights and liberties are respected.

19 Hernandez-Lopez v. State, 319 Ga. App. 662, 738 S.E.2d 116, Court of Appeals of Georgia (2013) https://cite.case.law/ga-app/319/662

20 Traft v. Commonwealth, 539 S.W.3d 647 Supreme Court of Kentucky (2018) https://cite.case.law/ga-app/319/662

21 Green v. City and County of San Francisco, No. 11-17892, United States Court of Appeals for the 9th Circuit (2014). https://law.justia.com/cases/federal/appellate-courts/ca9/18-10341/18-10341-2020-05-04.html

1035

Conclusion

As stated in the introduction, this product contains suggestions and recommendations, which, if adopted, will maximize ALPR technology's effectiveness while ensuring it is used ethically and responsibly. While this product provides a robust evaluation of the technology, it is impossible to cover every aspect of the technology. Therefore, the Working Group recommends that law enforcement use the tenets discussed in this document to help evaluate decisions regarding the use of ALPR technology. This must include the potential impact of ALPR technology on public trust and the community served. It is essential that, when implementing any technology program, law enforcement operate in a manner that is thoughtful, disciplined, and contextually mindful of its constituencies.

For those agencies wishing to implement an ALPR program but are still determining how to move forward, collaboration with other entities who have already developed robust, responsible programs is recommended. The sharing of best practices in crime-fighting technology among law enforcement has a history of beneficial impacts. Law enforcement must be good stewards of information and policies and be willing to share this with fellow law enforcement agencies wishing to begin using ALPR.

Law enforcement's use of ALPR is ubiquitous because the information these systems provide is advantageous. ALPR data has aided in countless successful criminal investigations and has proven to be one of the most valuable technologies available to law enforcement. Few technologies have aided law enforcement in keeping communities safe like ALPR. However, the capabilities of ALPR technology are continuously evolving, and the MCCA will continue to monitor it. The MCCA will remain engaged with all interested stakeholders and communicate the latest information with member agencies and the entire law enforcement profession so best practices can be adjusted as needed.

Acknowledgments

Major Cities Chiefs Association would like to extend a special thanks to the ALPR Working Group and its members listed below. The contents of this document would not be possible without the collaboration between these law enforcement professionals and the technology vendor participants.

Kelly Bluth
DETECTIVE
Las Vegas Metropolitan Police Department

Blake Bullock
SENIOR DIRECTOR & GM FLEET PRODUCTS
Axon

Paige Burley
CLIENT FACING DEPLOYMENT
Peregrine

Gabriel Candelaria
LIEUTENANT
Dallas Police Department

Jeffrey Carroll
ASSISTANT CHIEF OF POLICE
Metropolitan Police Department Washington D.C.

Laura Cooper
EXECUTIVE DIRECTOR
Major Cities Chiefs Association

Travis Eicher
LMPD TECHNICAL SERVICES
Louisville Police Department

Dan Gillespie
TECHNOLOGY PROGRAM MANAGER
Louisville Police Department

Jeremy Harrison
MAJOR
Oklahoma City Police Department

Kyle Hoertsch
PRODUCT DEVELOPMENT MGR ENTERPRISE SOLUTIONS
Motorola Solutions

Milton Wyatt Martin
ASSISTANT CHIEF
Houston Police Department

Matt Melton
SENIOR BUSINESS DEVELOPMENT MANAGER
Amazon Web Services

Jason Olin
DIRECTOR OF GOVERNMENT AFFAIRS
Major Cities Chiefs Association

Samuel Paul
DEPUTY
Los Angeles Sheriff's Department

Christian Quinn
MANAGING PRINCIPAL
Fulcrum Innovation LLC

Jeremy Slavish
SENIOR BUSINESS DEVELOPMENT MANAGER
Amazon Web Services

Paul Steinberg
SENIOR VICE PRESIDENT OF TECHNOLOGY
Motorola Solutions

Josh Thomas
VP OF POLICY AND COMMUNICATIONS
Flock Safety

Matthew Thomas
COMMANDER
Indianapolis Metropolitan Police Department

Mark Torres
COMMANDER - REAL TIME CRIME CENTER
Albuquerque Police Department

Mike Wagers
SENIOR VICE PRESIDENT STRATEGIC INITIATIVES
Axon

Dalton Webb
DIRECTOR OF RTCC STRATEGY
Flock Safety

Paden Weber
INTELLIGENCE OFFICER
Las Vegas Metropolitan Police Department

William Zelms
CAPTAIN
Virginia Beach Police Department

GRAPHIC DESIGN BY PADEN WEBER

1037

Definitions

Automated License Plate Reader/Recognition (ALPR): ALPR systems comprise cameras that capture an image of a vehicle's license plate and use Optical Character Recognition (OCR) to automatically read license plate characters.

Contextual Photo/Image: An overview image of the area around a detection.

ALPR Record/Detection: Is generated when an instance of a vehicle license plate is detected, imaged, and processed to identify the plate.

Hit: A detection of a license plate that matches a plate previously registered on a hotlist or hotplate.

Hotlist: A file that contains the license plate numbers of stolen vehicles; AMBER, SILVER, or other law enforcement alerts; lists of license plate numbers known to be associated with specific individuals, such as wanted or missing individuals.

Hotplate: A license plate with a wanted status. It may also be entered into a system designed to provide a notification of future detections.

Misread: An incorrect translation of a license plate.

Fixed Camera: An ALPR camera that is affixed to a non-moving structure.

Mobile Camera: A vehicle-mounted camera.

Law Enforcement Data: ALPR data collected by law enforcement-owned ALPR cameras.

Data Retention: Refers to the amount of time that the collected data will be preserved.

Personally Identifiable Information (PII): Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.[1]

National Crime Information Center (NCIC): An electronic clearinghouse of crime data, such as mug shots and crime records, available to virtually every criminal justice agency nationwide.[2]

1 Guidance on the Protection of Personally Identifiable Information, U.S. Department of Labor. https://www.dol.gov/general/ppiihttps://www.dol.gov/general/ppii

2 National Crime Information Center (NCIC), Federal Bureau of Investigation. https://le.fbi.gov/informational-tools/ncic

Appendix A – Success Stories

Homicide

After committing a homicide, the suspect fled the scene by vehicle. During the investigation, investigators learned that the suspect drove a specific vehicle with damage to the body. Using the ALPR system, detectives created a geographic boundary around the crime location. While reviewing the historical ALPR detections from that immediate area, a vehicle matching the suspect's vehicle description was identified. Detectives then discovered the actual license plate registration information, which returned to the primary suspect. Another query of that vehicle through the ALPR system revealed that the suspect vehicle had fled the jurisdiction immediately after the homicide occurred. This was later confirmed and corroborated by the suspect's cell phone location records.

Homicide

During a road rage incident resulting in a shooting and murder, the suspect was reportedly driving a black hearse. Responding officers obtained the victim's license plate number and checked it through the ALPR system. The officers located an ALPR record of the victim's vehicle passing an ALPR deployment site three minutes before the shooting. The officers checked for other vehicles driving past the ALPR cameras around the same time as the victim. The vehicle driving directly behind the victim was a black hearse. The ALPR data, along with a tip from the public, were pivotal in the arrest. The suspect gave a full confession. The arrest occurred within only a few hours of the crime.

Homicide

The victim knocked on the suspect's hotel room door. Annoyed by the knocking, the suspect opened the door and immediately shot and killed the victim. Surveillance footage of the suspect and his associate leaving captured the type of vehicle used by the suspect but did not capture the license plate. An ALPR camera system was stationed just down the street from the hotel. Officers reviewed the ALPR database for the time frame around the homicide. One minute before the 911 call, the ALPR camera captured a detection of a vehicle matching the one observed in the hotel surveillance. Armed with the vehicle registration information, the vehicle's lien holder was contacted, which provided new investigative leads. Within 11 hours of the shooting, officers located the suspect's vehicle hidden in a home's garage. The suspect and his associate were detained, provided a confession, and later charged with homicide.

Burglary

A police agency used ALPR to identify two suspect vehicles involved in a burglary. Multiple suspects in two vehicles committed a residential burglary, with the resident shooting and killing one of the suspects. Doorbell camera videos were recovered, and homicide detectives used them to establish a timeline. ALPR searches focused on the timeline, which resulted in ALPR scans for both suspect vehicles. A subject associated with one of the vehicles was later determined to be involved and arrested for burglary.

Sexual Assault and Attempted Murder

A victim met the suspect at a bar. They left and the suspect drove them to the desert, where he sexually assaulted, beat, strangled, and ran her over. The vehicle plate from the bar where the incident began was queried in the ALPR system. Historical detections placed the suspect vehicle in the desert where the victim was assaulted and left behind, along with other areas where the victim reported they had driven before the assault. The ALPR data was critical in the arrest of this violent attacker.

Fatal Hit-and-Run Traffic Accident

ALPR was used to identify the suspect vehicle that left the scene of a fatal traffic accident after hitting two people. The make and model of the vehicle were identified but not the license plate. The license plate and other supporting evidence were discovered by leveraging the ALPR system. After the crime occurred, ALPR detection records showed significant damage to the suspect vehicle.

Kidnapping

A male subject attempted to grab a female in a business parking lot. Video surveillance captured the subject and his vehicle. Detectives used video footage to determine the suspect vehicle's make, model, and year range. A query of the ALPR system provided sufficient information to confirm the suspect vehicle and registration. The male was later identified. A records check revealed he had two prior arrests for sexual assaults. He was later located and arrested for the crime of kidnapping.

Arson

A subject set fire to the sign and lawn outside an FBI office building. Surveillance footage showed a gold Chevy Tahoe with distinctive damage to the passenger and rear sides of the vehicle. The license plate number was not visible. Analysts searched more than 6,000 images in the ALPR database, looking for Chevrolet SUVs similar to the one in the surveillance footage. After searching the ALPR database, analysts found a vehicle with matching damage, identified the registered owner, then disseminated a bulletin for officers to locate the vehicle. Initially, officers could not locate the registered owner, who was transient. A few days later, a patrol officer spotted the vehicle based on the bulletin and detained the suspect. The suspect was positively identified and linked to the original arson and another one in a different part of the state. Less than one month later, the suspect accepted the criminal prosecution agreement offered by the prosecutors.

1040

Appendix B – Myths and Misconceptions

A review of case law provides a snapshot of the legalities supporting the use of ALPR technology. In contrast, some misinformation exists on the use of ALPR technology by law enforcement. Therefore, reviewing and understanding the myths and misconceptions about ALPR in law enforcement is essential.

MYTH

ALPR detections contain private, personally identifying information.

REALITY

ALPRs are designed to capture three details when a vehicle passes through their view: a photograph of the vehicle, the characters on the license plate of the vehicle, and the location, date, and time when the vehicle passes the ALPR.

Publicly-owned ALPR systems read the license plates of vehicles on public roadways and capture information that is generally not considered private. For example, if an individual were to stand by the side of a public road and take a picture of every vehicle that passed them, write down its plate number, and record the date and time, they would be within their legal rights to do so. Likewise, a person could place a camera on their property facing a public throughway and capture the same information an ALPR does. In *U.S. v. Ellison (2006)*, the Court explained that not only is there no privacy interest in a license plate number, but a subsequent entry into a computer system to retrieve other non-private information does not constitute a search.[3] By states mandating each vehicle operating on the roadway publicly display a license plate and even illuminate it at night, the expectation is for the license plate to be read at any time while on a public roadway.

An ALPR system does not automatically capture or record restricted information contained in an individual's motor vehicle records, such as their name, address, phone number, Social Security Number, driver identification number, etc. *The Driver's Privacy Protection Act of 1994* requires all states to protect this personal information ensuring ALPR reads are anonymous until additional steps are taken to access separate statutorily regulated databases. Therefore, when a law enforcement officer needs to access motor vehicle records based on data captured by an ALPR, they would need to perform the same manual processes to retrieve this information as they would in other investigative circumstances. Additionally, adequate policies limit access to ALPR data by requiring justification for the review of individual ALPR records. This effectively ensures that most ALPR-captured data is never even accessed before it is purged.

Therefore, retrieving non-public information based on ALPR data requires law enforcement to adhere not only to the policies and laws regarding the ALPR data but also to the policies and laws for accessing the restricted databases housing driver's license and vehicle information. In summary, ALPR systems do not grant expanded access to any non-public records databases, nor do they circumvent the auditing processes that are in place to ensure restricted data is accessed only for official use and as permitted by law.

3 United States v. Ellison, 462 F.3d 557, 561, United States Supreme Court. (6th Cir. 2006). https://caselaw.findlaw.com/la-court-of-appeal/1717448.html

1041

MYTH

ALPR technology is a form of mass surveillance.

REALITY

Guided by proper policy and processes, ALPRs are effective tools for law enforcement to narrow the focus of investigations and limit negative collateral impacts when policing high-crime areas.

A scenario most major city police departments are familiar with is as follows: A motorist is stopped by police only to later be released and sent on their way in a case of mistaken vehicle identity. Their misfortune was caused by driving a vehicle matching the general description of one recently broadcasted of a suspect vehicle in a violent crime. Though the detention is usually short-lived, the trauma it causes may not be. This type of "wrong place, wrong time" scenario is most likely to occur when non-specific or incorrect information is relayed to officers during an in-progress incident. Even a single negative experience like this can spread quickly throughout a community, jeopardizing efforts to build trust. Unfortunately, these scenarios most commonly affect residents in neighborhoods disproportionately impacted by violent crime and gun violence. The use of ALPRs can help mitigate these occurrences.

ALPRs provide an additional mechanism to corroborate or refute witness accounts of suspect vehicles. This helps narrow the focus of law enforcement when canvassing and provides officers with the increased ability to bypass lookalike vehicles and only interact with the cars that truly contain the distinct characteristics of the vehicle suspected in the crime.

A common talking point designed to instill fear in ALPRs technology is that they "could" be used to track people involved in first amendment protected activities. The purpose of robust agency policy is to restrict use to legally permissible actions and ensure accountability if rules are broken. It must be noted that the same policies and laws governing law enforcement's actions without technology still apply when using technology. In fact, the audit trails in technology ensure that a hindsight review of any actions taken is afforded an even more detailed perspective than the actions taken without records produced by technology.

Appendix C – State-Level Laws and Regulations

At least 16 states have statutes regarding the use of ALPR or the retention of data collected by ALPR technology. This information was derived from a database maintained by the National Conference of State Legislatures.[4] The states and their laws are as follows:

Arkansas-Ark. Code §§ 12-12-1801 to 12-12-1808

Prohibits use of ALPRs by individuals, partnerships, companies, associations or state agencies. Provides exceptions for limited use by law enforcement, by parking enforcement entities or for controlling access to secure areas. Prohibits data from being preserved for more than 150 days.

California-Calif. Veh. Code § 2413

Provides that the California Highway Patrol (CHP) may retain data from a license plate reader for no more than 60 days, unless the data is being used as evidence in felony cases. Prohibits selling or making available ALPR data to non-law enforcement officers or agencies. Requires CHP to report to the legislature how ALPR data is being used.

California-Calif. Civil Code §§ 1798.29, 1798.90.5

Establishes regulations on the privacy and usage of automatic license plate recognition (ALPR) data and expands the meaning of "personal information" to include information or data collected through the use or operation of an ALPR system. Imposes privacy protection requirements on entities that use ALPR information, as defined; prohibit public agencies from selling or sharing ALPR information, except to another public agency, as specified; and require operators of ALPR systems to use that information only for authorized purposes.

Colorado-Colo. Rev. Stat. § 24-72-113

Requires that video or still images obtained by passive surveillance by governmental entities, such as images from monitoring cameras, must be destroyed within three years after the recording of the images. Specifies that the custodian of a passive surveillance record may only access the record beyond the first anniversary after the date of creation of the record if there has been a notice of claim filed, or an accident or other specific incident that may cause the passive surveillance record to become evidence in any civil, labor, administrative, or felony criminal proceeding. Creates exceptions allowing retention of passive surveillance records of any correctional facility, local jail, or private contract prison and passive surveillance records made or maintained as required under federal law.

Florida-Fla. Stat. § 316.0777

Creates a public records exemption for certain images and data obtained through the use of an automated license plate recognition system and personal identifying information of an individual in data generated from such images. Provides that images and data containing personal information obtained from automated license plate recognition systems are confidential. Allows for disclosure to criminal justice agencies and to individuals to whom the license plate is registered in certain circumstances.

Georgia-Ga. Code § 35-1-22

License plate data may be collected and accessed only for a law enforcement purpose. The data must be destroyed no later than 30 months after it was originally collected unless the data are the subject matter of a toll violation or for a law enforcement purpose. Allows sharing of captured license plate data among law enforcement agencies. Law enforcement agencies deploying an automated license plate recognition system must maintain policies for the use and operation of the system, including but not limited to policies for the training of law enforcement officers in the use of captured license plate data. License plate data collected by a law enforcement agency is not subject to public disclosure.

4 Automated License Plate Readers: State Statutes," National Conference of State Legislatures. https://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx

Maine-29-A M.R.S.A. § 2117-A(2)

Prohibits the use of automatic license plate recognition systems except for certain public safety purposes. Provides that data collected is confidential and may be used only for law enforcement purposes. Data collected may not be stored more than 21 days.

Maryland-Md. Public Safety Code § 3-509

Specifies the procedures and protocols that a law enforcement agency must follow in connection with the operation of an "automatic license plate reader system" and "captured plate data." Requires the State Police to adopt procedures to address who has access to the data and training for those individuals and to create an audit process. Provides that data gathered by an automatic license plate reader system are not subject to disclosure under the Public Information Act.

Minnesota- Minn. Stat. §§ 13.82,13.824, 626.8472

Relates to data practices; classifies data and provides procedures related to automated license plate readers; provides the data that may be collected by such readers; relates to requirements for the sharing of such data among law enforcement agencies; requires the maintenance of a public log recording the uses of such data; requires related records maintenance and the auditing of such records; requires written procedures governing access to the data; requires certain notification when setting up readers.

Montana-Mont. Code Ann. §§ 46-5-117 to -119

Prohibits the use of license plate readers by an agency or employee of the state or any subdivision of the state on any public highway. Provides exceptions for specific agencies or purposes, such as state or local law enforcement, if specified requirements are met. Except as provided, license plate data captured by law enforcement may not be preserved for more than 90 days after the date that the data is captured.

Nebraska- Neb. Rev. Stat. § 60-3201 to 3209

Requires any governmental entity that uses an automatic license plate reader (ALPR) system to adopt a policy governing use of the system. Governmental entities also must adopt a privacy policy to ensure that captured plate data is not shared in violation of this act or any other law. The policies must be posted on the internet or at the entity's main office. Requires annual reports to the Nebraska Commission on Law Enforcement and Criminal Justice on ALPR practices and usage. Provides that captured plate data is not considered a public record.

New Hampshire-N.H. Rev. Stat. Ann. §§ 261.75-b, 236.130

Restricts the use of automated license plate readers to local, county and state law enforcement officers, who shall only use the devices subject to specified conditions and limitations and for specified purposes. Provides that records of number plates read shall not be recorded or transmitted anywhere and shall be purged from the system within 3 minutes of their capture, unless the number resulted in an arrest, a citation or protective custody or identified a vehicle that was the subject of a missing or wanted person broadcast.

North Carolina-N.C. Gen. Stat. §§ 20-183.30 to .32

Requires state or local law enforcement agencies to adopt a written policy governing the use of an ALPR system that addresses databases used to compare data obtained by the system, data retention and sharing of data with other law enforcement agencies, system operator training, supervision of system use, and data security and access. Requires audits and reports of system use and effectiveness. Limits retention of ALPR data to no more than 90 days, except in specified circumstances. Provides that data obtained by the system is confidential and not a public record.

Oklahoma-Okla. Stat. §§ 47-4-606.1

Provides that participating law enforcement agencies may use automatic license plate reader systems to access and collect data for the investigation, detection, analysis or enforcement of the state's compulsory insurance law. States that data collected under the program may not be used by any individual or agency for purposes other than enforcement of the compulsory insurance law, prohibits sale of the data under the program, and provides that data is exempt from the Oklahoma Open Records Act, except when retained as evidence of a violation of the compulsory insurance law. These provisions do not prohibit the use of any other automated license plate reader system by an individual or private legal entity for lawful purposes.

Tennessee-Tenn. Code §§ 55-10-302, 10-7-504(a)

Provides that any captured automatic license plate data collected by a government entity may not be stored for more than 90 days unless they are part of an ongoing investigation, and in that case provides for data to be destroyed after the conclusion of the investigation. Captured plate data from automatic license plate reader systems must be treated as confidential and shall not be open for inspection by members of the public.

Utah-Utah Code §§ 41-6a-2001 to -2005

Provides that a governmental entity may not use an automatic license plate reader system except for specified uses, such as by law enforcement agencies for the purpose of protecting public safety or conducting criminal investigations and by other government entities for limited other purposes. Provides that captured plate data are a protected record under the Government Records Access and Management Act, if the captured plate data are maintained by a governmental entity. Provides that captured plate data may only be shared for specified purposes, may only be preserved for a certain time and may only be disclosed pursuant to specific circumstances such as a disclosure order or a warrant. Government entities may not use privately held captured plate data without a warrant or court order, unless the private provider retains captured plate data for 30 days or fewer. Allows an institution of higher education to use automatic license plate readers under certain circumstances.

Vermont- 23 V.S.A. §§ 1607, 1608

Requires a law enforcement officer to be certified in the use of an automated license plate reader to operate such a system. Provides that active system data may only be accessed by an officer with a legitimate law enforcement purpose for the data. A legitimate purpose includes a person's defense against certain charges and does not include enforcement of parking or traffic violations other than commercial motor vehicle violations. Limits retention and access to information gathered through the use of an ALPR system. Requires the Department of Public Safety to adopt rules to implement the law. Requires the Auditor of Accounts to examine requests for data to determine whether the request and the release complied with the law.

1045

Appendix D – CJIS Security Policy

Agencies that wish to use the CJIS Security Policy to assess the security practices of a service provider that will be handling ALPR data should consider the following sections:

- Private Contractor User Agreements and FBI-CJIS Security Addendum [5.1.5]: Private contractors who perform criminal justice functions for a Criminal Justice Agency (CJA) shall be permitted to access CJI pursuant to an agreement between the CJA and the contractor that incorporates the FBI-CJIS Security Addendum approved by the Director of the FBI.
- Agency User Agreements [5.1.1.6]: Fingerprint-based background checks and written agreement with the agency when required.
- Secondary Dissemination [5.1.3]: If data is released to another authorized agency and not part of a primary information exchange agreement, this shall be logged.
- Security Awareness Training [5.2]: All personnel with access to CJI (Criminal Justice Information) shall receive security awareness training within six months of assignment, and biennially thereafter.
- Security Training Records [5.2.3]: Records of security awareness training shall be kept current and maintained by a Security Officer (CSO).
- Reporting Structure and Responsibilities [5.3.1.1]: Establishment of a primary Point of Contact (POC) for CJIS incident handling and response.
- Events [5.4.1.1]: Description of the events that must be logged within the system.
- Audit Monitoring, Analysis and Reporting 5.4.3]: Responsibility for review and analysis of audit records, at a minimum of once a week, to look for inappropriate or unusual activity.
- Audit Record Retention [5.4.6]: The agency shall retain audit records for at least one year.
- Least Privilege [5.5.2.1]: The agency shall approve individual access privileges and enforce the most restrictive set of rights and privileges needed by users for the performance of specified tasks. Logs maintain access privilege changes for a minimum of one year or at least equal to the agency's record retention policy, whichever is greater.
- Access Control Mechanisms 5.5.2.4]: One or more of the following must be employed: access control lists (users, groups, machines), resource restrictions (permission sets), encryption and strong key management, application-level access control.
- Unsuccessful Login Attempts [5.5.3]: CJIS Security Policy requires that after five consecutive invalid attempts, the account shall be locked out for a minimum of 10 minutes.
- System Use Notification [5.5.4]: The system shall allow a notification message to be displayed to let users know a) they are accessing a restricted system, b) usage is monitored, recorded and subject to audit, c) unauthorized use is prohibited and may result in penalties, and d) use of the system indicated consent to monitoring.
- Session Lock [5.5.5]: CJIS Security Policy requires that the system shall prevent access via a session lock after a minimum of 30 minutes of inactivity.
- Remote Access [5.6]: Rules for monitoring and controlling remote access via the internet.
- Use of Originating Agency Identifiers in Transactions and Information Exchanges [5.6.1.1]: An FBI-issued ORI number shall be assigned at the agency level and attached to all activities by the agency's users.
- Password [5.6.2.1.1]: Requirements and standards for passwords.
- Personal Identification Numbers [5.6.2.1.2]: Best Practices on PIN use.
- Advanced Authentication [5.6.2.2]: Advanced Authentication requirements.
- Identifier Management [5.6.3]: Requirements of agencies to manage user identifiers.
- Network Diagram [5.7.1.2]: Requirements for a network topological diagram.

1046

- Media Protection [5.8]: Requirements for security and protection of electronic and physical media.
- Physical Protection [5.9]: Requirements for physical security and access controls around all hardware, software and media.
- System and Communication Protection and Information Integrity [5.10]: Prevent CJI from being transmitted unencrypted across the public network.
- Boundary Protection [5.10.1.1]: Ensure that failure of boundary protection mechanisms do not result in unauthorized release of information.
- Encryption [5.10.1.2]: Minimum of 128 bit encryption when CJI data is transmitted beyond the physical security boundary.
- Intrusion Detection Tools and Techniques [5.10.1.3]: Requirements for intrusion detection tools.
- Cloud Computing [5.10.1.5 and Appendix G.3]: Recommendations for use of cloud computing and assessment of cloud computing service providers.
- Partitioning and Virtualization [5.10.3]: Requirements for partitioning of data and virtualization of resources.
- Patch Management [5.10.4.1]: Requirements for management of software patches.
- Malicious Code Protection [5.10.4.2]: Virus Protection requirements.
- Spam and Spyware Protection [5.10.4.3]: Spam and Spyware Protection requirements.
- Security Alerts and Advisories [5.10.4.4]: Guidance for alerts and advisories.
- Personnel Security [5.12]: Fingerprint-based background checks and rules based on findings.
- Personnel Termination [5.12.2]: Terminated employees shall immediately have access revoked.
- Personnel Sanctions[5.12.3]: Process for employees failing to comply with security policies.
- Mobile Devices [5.13]: Where appropriate, the technology partner must support the agency's mobile device practices (patch management, etc.)

1047

Appendix E – ALPR Audit and Transparency Report Template

The following template provides a rudimentary example of the details and considerations in providing a published report about the performance and effectiveness of an ALPR program.

Automated License Plate Reader Program
Annual Transparency Report

Introduction

The introduction should provide context and background as to what the report is addressing. The introduction defines the specific objectives and purpose of the report. It indicates any problems that may exist and provides answers to problems explored. Finally, the introduction will preview the report and outline the report structure.

Discussion

This is the main body of the report, and it has two primary purposes. The first is to share and explain the conclusions. The second is to justify any recommendations that may be made in the report.

Specific data points that may be considered:

- Number of detections
- Number of hotplate hits
- Number of queries conducted by users
- Number of arrests directly related to ALPR
- Number of user-generated hotplates
- Breakdown of hotplate hit types
- Year-over-year analysis and trends

Conclusion

This section should relate to the information shared in the report. It should be specific to the objectives of the report. It may also address any issues that may be interpreted from the information shared. The conclusion should be brief, logical, and specific.

Recommendations

Recommendations shared should point to future action that can be completed. Recommendations should be feasible, action-oriented and arranged in order of importance.

From: /O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=B4D5FFB1CAFC42EDA86DA25B38CD03DF-JENNIFER M.
To: Mawn, John (POL); Pinkham, John (POL); Cyr, Mark (POL)
Cc: Kelly, Siobhan (POL)
Subject: Legal Talking Points/Fed Cameras on MassDOT properties
Date: Wednesday, November 1, 2023 10:25:00 AM
Attachments: image001.png

Sirs:

As requested, below are some legal talking points regarding why MassDOT should allow MSP cameras on MassDOT properties as opposed to federal cameras:

1. MSP must adhere not only to federal law with regard to camera surveillance, it must also adhere to Massachusetts law, which is much more restrictive than federal law. For example, in the case of Commonwealth v. McCarthy, 484 Mass. 493 (2020), the SJC adopted the "mosaic theory" when it comes to surveillance cameras, which holds that "with 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." Federal agencies are not bound by MA law.

2. MSP requires all of its law enforcement partners who are given permission to access MSP cameras, including federal agencies, to adhere to its ALPR policy and all MA laws. MSP's ALPR policy is regarded as the leading ALPR policy in the state, and it incorporates MA case law. Most other state law enforcement agencies have adopted MSP's policy or have relied on our policy when drafting their own.

3. There is no guarantee a federal agency would give MSP or any other state law enforcement agency access to its cameras should its cameras be placed on MassDOT property, which would be a large impediment for state investigations.

Let me know if you have any questions.

Jennifer M. Staples
Chief Legal Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Tel: (508) 820-2307
Cell: [redacted] M.G.L. c. 4,sec. 7,cl.26 (n)(security)

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: Staples, Jennifer (POL)
To: Mawn, John (POL); Pinkham, John (POL); Cyr, Mark (POL)
Cc: Kelly, Siobhan (POL)
Subject: Legal Talking Points/Fed Cameras on MassDOT properties
Date: Wednesday, November 1, 2023 10:25:43 AM
Attachments: image001.png

Sirs:

As requested, below are some legal talking points regarding why MassDOT should allow MSP cameras on MassDOT properties as opposed to federal cameras:

1. MSP must adhere not only to federal law with regard to camera surveillance, it must also adhere to Massachusetts law, which is much more restrictive than federal law. For example, in the case of Commonwealth v. McCarthy, 484 Mass. 493 (2020), the SJC adopted the "mosaic theory" when it comes to surveillance cameras, which holds that "with 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." Federal agencies are not bound by MA law.

2. MSP requires all of its law enforcement partners who are given permission to access MSP cameras, including federal agencies, to adhere to its ALPR policy and all MA laws. MSP's ALPR policy is regarded as the leading ALPR policy in the state, and it incorporates MA case law. Most other state law enforcement agencies have adopted MSP's policy or have relied on our policy when drafting their own.

3. There is no guarantee a federal agency would give MSP or any other state law enforcement agency access to its cameras should its cameras be placed on MassDOT property, which would be a large impediment for state investigations.

Let me know if you have any questions.

Jennifer M. Staples
Chief Legal Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Tel: (508) 820-2307
Cell: [redacted] M.G.L. c. 4,sec. 7 cl.26 (n)(security)

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)
To: Donnelly, William
Subject: LPR MOU
Date: Tuesday, March 28, 2023 12:23:41 PM
Attachments: Raynham ALPR MOU Signed.pdf

Hi Sgt. Donnelly,

Attached is a signed copy of the ALPR MOU for your agency's records.

I received your voicemail and apologize for the delay; I have been tied up in court over the past couple weeks. The new software did not come with the desired features and capabilities, and we do not yet have the ability to provide tenant users direct access their data in the way we had hoped. This feature is promised to us in the next update cycle to be released at the beginning of May. I will keep you in the loop when I have that update.

Respectfully,

Noah

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

From: Grasso, Jimi (POL)
To: Cyr, Mark (POL)
Cc: Nunes, John (POL); Staples, Jennifer (POL); Wheeler, Mark (POL)
Subject: LPR Notes
Date: Wednesday, November 1, 2023 12:33:33 PM
Attachments: LPR MA DOT (Readers Digest Version) Talking Points.docx
MSP DHS DOT Collocation Request 7-23 Notes Update3 (1).doc
TRF-11 Automatic License Plate Recognition.pdf
Outlook-xmc03efc.png

LTC,

In preparation for Colonel Mawn's Thursday meeting with MA DOT. Please find three attachments; one is a "reader's digest" version of LPR talking points. The second is a 7/23 full version provided by Sgt. Pack. The third is the current MSP LPR Policy referenced from PowerDMS.

Please advise if you need anything further.

Respectfully submitted,

Major Jimi Grasso #2529
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Road Framingham, MA 01702
(office) 508-820-2661 / (mobile) [redacted]

Information contained in this email may be confidential and/or CORI. Receipt and/or dissemination by persons other than the intended addressee may be subject to criminal penalties.

From: Ross, Jonathan (POL)
To: POL-DL-GHQ Communications
Subject: LPR Policy
Date: Wednesday, June 28, 2023 6:51:11 AM
Attachments: TRF-11 Automatic License Plate Recognition (1).pdf

---

Everyone should be aware of this updated policy and sign off on it in PowerDMS.

Thanks,
Jon

From: Connolly, Kevin
To: Pack, Noah (POL)
Subject: LPR success story
Date: Tuesday, July 25, 2023 12:30:20 PM
Attachments: image004.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.

Noah,

I just wanted to pass along a quick success story we had here in Barnstable. On May 27, 2023 we had 2 unknown individuals fire several rounds at a motor vehicle in the Craigville Beach parking lot at 8:30pm as beachgoers were in the area enjoying a nice sunset. Although no one was hit, the vehicle was struck 5 times and the community was immediately put on edge because of this brazen violent act.

As we were developing suspects we were able to identify the vehicle and plate of the car used to help the shooters flee the scene. Utilizing CSLI for the suspected occupants and plate reads from Yarmouth, Barnstable, and Sagamore we were able to show the vehicle and the suspects traveling together prior to and immediately after the shooting. Having access to the plate readers in the other communities was invaluable in this investigation and helped solidify the probable cause needed to obtain arrest warrants for the responsible parties.

Thank you again for keeping these readers up and running, they truly help more than you know.

Kevin

Kevin A. Connolly
Detective Sergeant
Barnstable Police Department
Investigative Services Division
Digital Forensics & Investigations Unit
USSS New England Cyber Fraud Task Force
508-958-6522
connollyk@barnstablepolice.com

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Saturday, July 1, 2023 8:50 PM
To: Pack, Noah (POL) <noah.pack@state.ma.us>
Subject: LPR System User Updates

[EXTERNAL EMAIL] DO NOT CLICK links or attachments unless you recognize the sender and know the content is safe.

CAUTION: This email originated from outside your organization. Exercise caution when opening attachments or clicking links, especially from unknown senders.

Hello Boss4 users, please see the updates below regarding the Department's ALPR system.

Policy Update

The Department's ALPR policy (TRF-11) was officially updated as of June 27, 2023. An updated copy is attached to this email. This policy governs the use of the Department's ALPR systems by sworn and civilian members of MSP and our partner agencies who have completed MOUs with us. Please review it to ensure you are familiar with the most recent version. Many of the updates to this policy directly reflect the best practices that we have already been doing and teaching, such as limiting the scope of searches and the duration of manual hotlist entries.

One noteworthy update is that a manual hotlist entry request must be authorized by a supervisor, except in exigent circumstances/emergencies. This can be satisfied in one of two ways: (1) the request can come directly from a supervisor (Sgt. or above or civilian equivalent), or (2) the requestor can provide the name of the supervisor who has authorized the request.

Hotlist Entries

When entering a plate on a hotlist, information must be entered in the free text fields about the vehicle, the reason for the entry, the date of the entry, and who entered it. Please do not enter just a plate. For investigations, include enough information to identify what vehicle and case it refers to. For public safety entries, include enough info so that someone receiving the alert would know what to do or who to call if it alerts them. For all entries, there must be enough info so that we can identify an authorized use and specific case or incident when conducting an audit. An example of a solid entry would be:

LPN: 123ABC
Field 1: 2020
Field 2: Toyota
Field 3: Highlander
Field 4: White
Field 5: Entered 5/1/23 by #1234
Field 6: Homicide invest [OR] New Bedford kidnapping
Field 7: 2023-123-123 [OR] Contact New Bedford PD

Expiration dates: Manual hotlist entries must have an initial expiration date of no longer than 30 days and must be removed as soon as the information become invalid or is no longer needed for the investigation. For entries requested by a dispatch entity or for other short-term matters, such as a general BOLO, the entries must be set to expire no later than the following day (generally 24-48 hours). The intent of this is to avoid a plate being left on the hotlist for long after the short-term incident is resolved.

Searches:

When conducting a search, please be mindful of the temporal and geographic parameters that are reasonable and consistent with the needs of the investigation or incident. In short, this means to ask how much historical time and how much area (how many cameras) do we need to search, as these are among the questions being asked in court when assessing the reasonableness of LPR use in a particular case.

Historical data visibility is currently limited to **90 days**, but data is retained for 1 year by DCJIS policy. If you need to search further back than 90 days, please contact the Commonwealth Watch Center for assistance at fusion@mass.gov.

Successes:

LPR continues to provide critical information for major incidents and investigations, from shootings to kidnappings, all over the Commonwealth. Please continue to forward these success stories to me or the Watch Center to help us document and defend the public safety value of this system. Feel free to also forward any suggestions on how we might improve the system.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

From: Pack, Noah (POL)
To: Pack, Noah (POL)
Subject: LPR System User Updates
Date: Saturday, July 1, 2023 8:50:24 PM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

Hello Boss4 users, please see the updates below regarding the Department's ALPR system.

Policy Update

The Department's ALPR policy (TRF-11) was officially updated as of June 27, 2023. An updated copy is attached to this email. This policy governs the use of the Department's ALPR systems by sworn and civilian members of MSP and our partner agencies who have completed MOUs with us. Please review it to ensure you are familiar with the most recent version. Many of the updates to this policy directly reflect the best practices that we have already been doing and teaching, such as limiting the scope of searches and the duration of manual hotlist entries.

One noteworthy update is that a manual hotlist entry request must be authorized by a supervisor, except in exigent circumstances/emergencies. This can be satisfied in one of two ways: (1) the request can come directly from a supervisor (Sgt. or above or civilian equivalent), or (2) the requestor can provide the name of the supervisor who has authorized the request.

Hotlist Entries

When entering a plate on a hotlist, information must be entered in the free text fields about the vehicle, the reason for the entry, the date of the entry, and who entered it. Please do not enter just a plate. For investigations, include enough information to identify what vehicle and case it refers to. For public safety entries, include enough info so that someone receiving the alert would know what to do or who to call if it alerts them. For all entries, there must be enough info so that we can identify an authorized use and specific case or incident when conducting an audit. An example of a solid entry would be:

LPN: 123ABC
Field 1: 2020
Field 2: Toyota
Field 3: Highlander
Field 4: White
Field 5: Entered 5/1/23 by #1234
Field 6: Homicide invest [OR] New Bedford kidnapping
Field 7: 2023-123-123 [OR] Contact New Bedford PD

Expiration dates: Manual hotlist entries must have an initial expiration date of no longer than 30 days and must be removed as soon as the information become invalid or is no longer needed for the investigation. For entries requested by a dispatch entity or for other short-term matters, such as a general BOLO, the entries must be set to expire no later than the following day (generally 24-48 hours). The intent of this is to avoid a plate being left on the hotlist for long after the short-term incident is resolved.

Searches:

When conducting a search, please be mindful of the temporal and geographic parameters that are reasonable and consistent with the needs of the investigation or incident. In short, this means to ask how much historical time and how much area (how many cameras) do we need to search, as these are among the questions being asked in court when assessing the reasonableness of LPR use in a particular case.

Historical data visibility is currently limited to **90 days**, but data is retained for 1 year by DCJIS policy. If you need to search further back than 90 days, please contact the Commonwealth Watch Center for assistance at fusion@mass.gov.

Successes:

LPR continues to provide critical information for major incidents and investigations, from shootings to kidnappings, all over the Commonwealth. Please continue to forward these success stories to me or the Watch Center to help us document and defend the public safety value of this system. Feel free to also forward any suggestions on how we might improve the system.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

From: Pack, Noah (POL)
To: Joseph Molloy
Subject: LPR System
Date: Friday, May 26, 2023 3:39:12 PM
Attachments: ALPR TENANT MOU 2023.docx
TRF-11 Nov21.pdf

Good afternoon Joe,

We now have the ability for outside agency users to be able to view data from cameras in their jurisdiction. Attached is a copy of the MOU and our current ALPR policy. If this is acceptable to your agency, please sign and return to us. We can then set up a training for a few members of your agency to get access.

All users must receive training, and we do not have the resources to manage a large or a constantly changing pool of users (this applies to our own staff as well). Therefore please select approximately 2-4 users from your agency (we recommend investigations level staff primarily due to their experience).

The training is tentatively scheduled for **June 7 at 10:00 AM**. It will take place remotely via Teams and will take about 1.5 hours. Users should ideally be at their computers and able to follow along. When available, please send me the names and email addresses of the users selected by your agency.

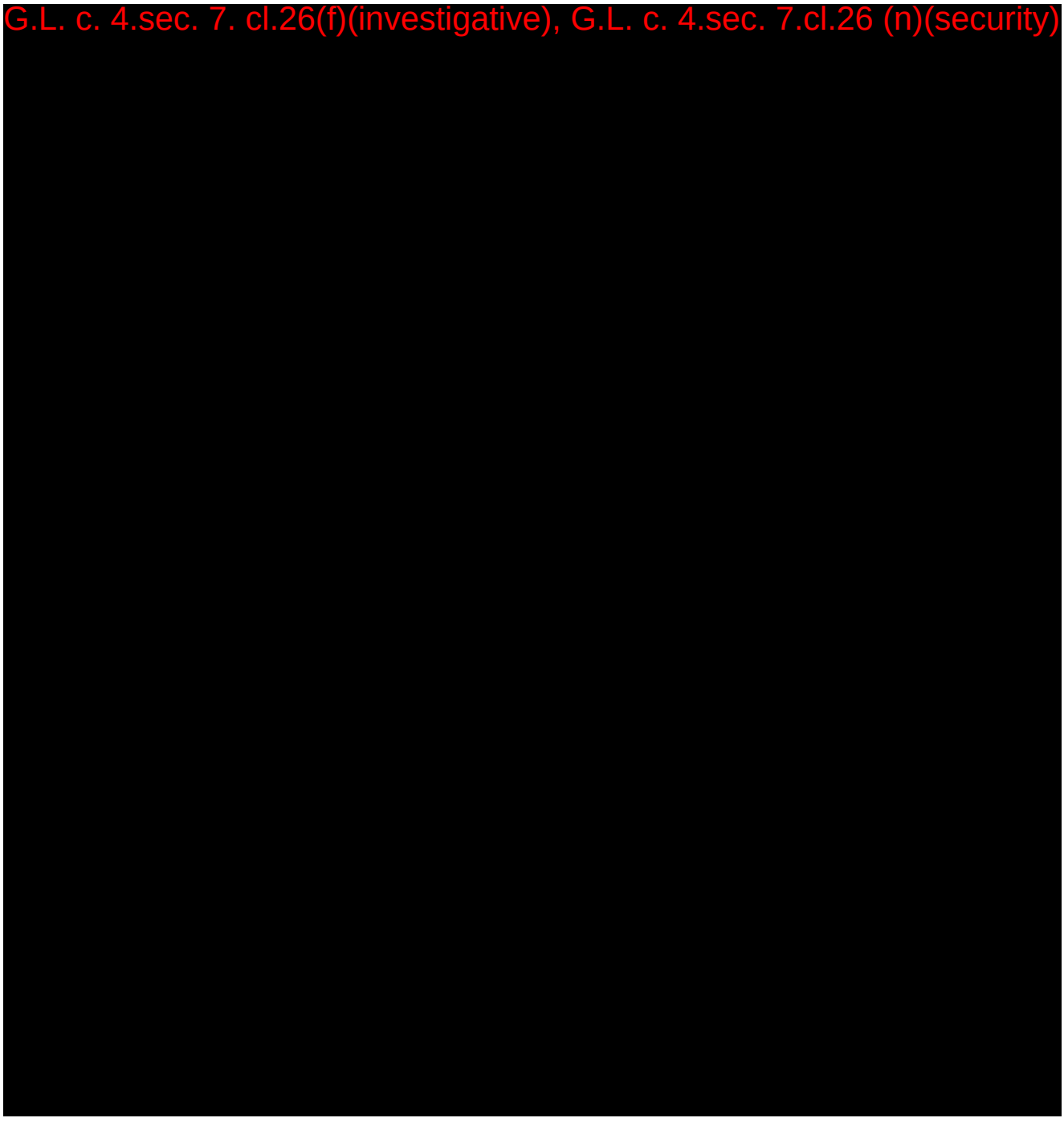
Respectfully,

Noah

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

From: Pack, Noah (POL)
To: Bender, Sean (POL); Bennett, Marcy (POL); Brooks, Brian (POL); Franquiz, Andrew (POL); Grunewald, Brady (POL); Lee, James (POL); Lopez, Adrian (POL); Mccarron, Richard (POL); O"Hara, Edward (POL); Palmer, David (POL); Peterson, Kaitlyn H. (POL); Salvatore, Justin (POL)
Cc: Tucker, Daniel T (POL); Rudolph, James (POL)
Subject: LPR Updates
Date: Saturday, July 1, 2023 8:25:59 PM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

Motorola/Vigilant LEARN



The Department's ALPR policy (TRF-11) was officially updated as of June 27, 2023. This policy governs the use of ALPR systems by sworn and civilian members. Please review it (attached) to ensure you are familiar with the most recent version. Many of the updates to this policy directly reflect the best practices that CWC has already doing, such as limiting the scope of searches and the duration of manual hotlist entries. The section titled "Search Procedures" would be particularly relevant to review.

One noteworthy update is that a manual hotlist entry request must be authorized by a supervisor, except in exigent circumstances/emergencies. This can be satisfied in two ways: (1) the request can come directly from a supervisor (Sgt. or above), or (2) the requestor can provide the name of the supervisor who has authorized the request. Until requestors get used to sending this info, you may find yourselves advising them of the requirement and asking for the supervisor's name. For example, something like this might work:

> "We have received your hotlist request. Pursuant to recent MSP policy updates, hotlist requests must be authorized by a supervisor. Please provide the name of the supervisor who has authorized this request."

ALPR Administrator

Thank you for your time and effort as we continue working to improve our Department's LPR system. Some of you know that I have been transferred to a new assignment, and DHS is in the process of selecting someone new to take over the ALPR Administrator role. I will continue to handle these duties through that transition, and as always please feel free to reach out with questions, comments, and success stories.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Investigative Services
Critical Incident Technical Investigations (CITI)

From: Pack, Noah (POL)
To: Daniel Wilburn
Date: Wednesday, October 18, 2023 9:51:33 PM
Attachments: PAGIS 2.15 MANUAL.pdf

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Investigative Services
Critical Incident Technical Investigations (CITI)

From: Pack, Noah (POL)
To: Daniel Wilburn
Date: Wednesday, October 18, 2023 9:48:20 PM
Attachments: PAGIS 2.14 MANUAL_ADMIN.pdf

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Investigative Services
Critical Incident Technical Investigations (CITI)

To: LASHAWN.BENTON2@USDOJ.GOV
Date: Wednesday, October 18, 2023 1:10:41 PM
Attachments: 2020 COPS AHTF GAM Oct 2023 FINAL.docx

Good afternoon:
We just submitted a GAM in just grants for 2020HPWX0004, Anti-Heroin Task Force 2020. I have attached the letter that was attached. My apologies, our prior grant manager was Judith Williford,

Rebecca Rust
Deputy Director of Grants and Special Projects
Massachusetts State Police
470 Worcester Road
Framingham, MA 01712
508-820-2688
Rebecca.Rust@pol.state.ma.us

Your feedback is important to us. We value your input to continuously improve and provide you with the best possible service.
Please let us know how we are doing by taking our short survey at the following link:
MSP Crime Laboratory Service Satisfaction Survey

All communications sent or received by this Commonwealth of Massachusetts email address may be subject to disclosure under the Massachusetts Public Records Law (M.G.L. Chapter 66, Section 10) and the Federal Freedom of Information Act.
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)
To: Walczak, Ryan (POL)
Date: Tuesday, September 5, 2023 12:32:51 PM
Attachments: DC Order ALPR Retention DRAFT.docx

DRAFT for your review, I made some tweaks to it.

From: Quigley, Robert (POL)
To: Quigley, Robert (POL)
Date: Thursday, August 31, 2023 9:07:31 AM
Attachments: bookmarks_6_1_23.html
_CFC On Call Guide.pdf
700cmr7 MASS DOT hotlist info.pdf
ACISS - UPDATE - Step-by-Step.pdf
ACISS Distribution_Step-by-Step (2).pdf
Boat camera operation.docx
Boss 4 Tutorial Brooks.pptx
BOSS LPR 4 Step-by-Step.pdf
Boston FLIR Camera Locations.xlsx
Capture - Typical distro list for dissemination.PNG
CFC duties.docx
CNC LIVE How to Create an Event.docx
CNC LIVE How to Create an Event.pdf
Copy of AET Toll Zone Plaza ID Codes.xlsx
Copy of Copy of Boat IP list.xlsx
HOW TO FIND THE NEAREST CRUISER ON GEO TAB.docx
Marine Unit Cameras.docx
PASS THROUGH examples.docx
protests.docx
SAR EXAMPLES.docx
SILVER ALERT MA DOT hot list request.docx
Sitrep examples - Justin.docx
SITREP EXAMPLES ACTUAL.docx
TTL Workflow DRAFT1 UPDATE5.pptx
Watch Center passwords.docx
Webstream distro 10-2021.docx
When to call Procopio.pdf
Work up - Fillable PDF - Template.pdf
image00001.png

<!--[if lte mso 15 || CheckWebRef]-->

Quigley, Robert (POL) has shared a OneDrive for Business file with you. To view it, click the link below.

bookmarks_6_1_23.html

<!--[endif]-->

Respectfully,

Lieutenant Robert P. Quigley Jr.
Massachusetts State Police
Commonwealth Fusion Center
470 Worcester Road
Framingham, MA 01702
508-820-2233

The preceding email message (including any attachments) contains information that may be confidential, may be protected by 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)
To: Walczak, Ryan (POL)
Date: Wednesday, July 19, 2023 6:22:20 PM
Attachments: LicensePlateReaderProgramBestPracticesGuide-October2021.pdf

---

Sergeant Noah H. Pack
Massachusetts State Police
Division of Investigative Services
Critical Incident Technical Investigations (CITI)

Date: Tuesday, June 27, 2023 3:00:37 PM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

Sups,

Please share the above policy with your dispatchers. Under the current policy, the Commonwealth Watch Center and the Commonwealth Fusion Center are the primary ALPR resources for the Department. Also, non-Department ALPR Systems accounts are prohibited unless approved by the Division Commander of Homeland Security and Preparedness, through chain of command.

If your center or any of its personnel have Department ALPR and/or non-Department ALPR access, please let me know by end-of-week so a determination can be made to

Kenneth E. Handfield, Jr.
Director of Dispatch Services

Massachusetts State Police
Communications Section, Dispatch Services Unit
50 Maple Street, Rm. 2330
Milford, MA 01757

Office: 508.820.2347
Cell & Text: [redacted]

Fax: 774.462.3768 (Milford)

Email: Kenneth.Handfield@Mass.gov

Date: Wednesday, May 31, 2023 1:40:48 PM
Attachments: TRF-11 Automatic License Plate Recognition DRAFT 2023 (1) (1).docx

---

Sgt. Christopher Condlin #2970
Strategic Planning and Analysis Section
Office of the Superintendent
508-988-7439

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.

Date: Tuesday, May 30, 2023 12:55:09 PM
Attachments: TRF-11 Automatic License Plate Recognition DRAFT 2023 (1) (1).docx

---

Sgt. Christopher Condlin #2970
Strategic Planning and Analysis Section
Office of the Superintendent
508-988-7439

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: Ben Miller
To: Bernstein, Eric (POL)
Subject: Mass Chiefs ; Elsag ALPR / Mass State Police ; MPH M7 spec sheet
Date: Friday, April 14, 2023 11:27:09 AM
Attachments: Spec Sheet Mobile Camera 2022 01 MPH M7 Elsag ALPR.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.

Hello Lieutenant,

It was a pleasure to speak with you at the Massachusetts Chiefs Show on Wednesday. As discussed, we would be pleased to offer our technology and customer service to improve your ALPR deployments.

Since your main interest is Mobile ALPR for your cruisers, please find attached a copy of our MPH (Mobile Plate Hunter) M7 (7th generation) Mobile ALPR system for your review.

I will send a follow up email which gives you an overview of our company plus our role in and dedication towards ALPR for Law Enforcement and look forward to speaking with you again at your earliest convenience.

Best Regards, Ben

Ben Miller
Operations Director New England
Selex ES Inc., a Leonardo Company
ELSAG® ALPR Plate Recognition Technology
Proudly Made in the USA
4221 Tudor Lane
Greensboro, North Carolina 27410 USA
ben.miller@leonardocompany-us.com
Cell: +1 [redacted]
www.elsag.com

The content of this email is confidential and intended for the recipient specified in message only. It is strictly forbidden to share any part of this message with any third party, without a written consent of the sender. If you received this message by mistake, please reply to this message and follow with its deletion, so that we can ensure such a mistake does not occur in the future.

From: Pack, Noah (POL)
To: Cyr, Mark (POL)
Subject: McCarthy
Date: Thursday, March 2, 2023 11:48:01 AM
Attachments: McCARTHY, COMMONWEALTH vs., 484 Mass. 493.pdf

Some salient points:

This court concluded that although the widespread use by Massachusetts police departments of
automatic license plate readers (ALPRs) could implicate constitutional protections against unreasonable searches, the positioning of four cameras in fixed positions on the ends of the two
bridges leading to Cape Cod did not provide a mosaic of location information that was sufficiently detailed to invade a reasonable expectation of privacy, and therefore, the limited use
of such ALPRs did not constitute a search within the meaning of art. 14 of the Massachusetts Declaration of Rights or the Fourth Amendment to the United States Constitution. [497-509] Gants, C.J., concurring.

-

We conclude that, while the defendant has a constitutionally protected expectation of privacy in the whole of his public movements, an interest which potentially could be implicated by the widespread use of ALPRs, that interest is not invaded by the limited extent and use of ALPR data in this case.

-

With 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. The one-year retention period indicated in the EOPSS retention policy certainly is long enough to warrant constitutional protection.

-

Of course, the constitutional question is not merely an exercise in counting cameras; the analysis should focus, ultimately, on the extent to which a substantial picture of the defendant's public movements are revealed by the surveillance. For that purpose, where the ALPRs are placed matters too. ALPRs near constitutionally sensitive locations -- the home, a place of worship, etc. -- reveal more of an

individual's life and associations than does an ALPR trained on an interstate highway. A network of ALPRs 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.

-

Similarly, with cameras in enough locations, the hot list feature could implicate constitutional search protections by invading a reasonable expectation of privacy in one's real-time location. If deployed widely enough, ALPRs could tell police someone's precise, real-time location virtually any time the person decided to drive, thus making ALPRs the vehicular equivalent of a cellular telephone "ping." .... Of course, no matter how widely ALPRs are deployed, the exigency exception to the warrant requirement would apply to this hot list feature.

-

The limited number of cameras and their specific placements, however, also are relevant in determining whether they reveal a mosaic of location information that is sufficiently detailed to invade a reasonable expectation of privacy. The cameras in question here gave police only the ability to determine whether the defendant was passing onto or off of the Cape at a particular moment, and when he had done so previously. This limited surveillance does not allow the Commonwealth to monitor the whole of the defendant's public
movements, or even his progress on a single journey. These particular cameras make this case perhaps more analogous to CSLI, if there were only two cellular telephone towers collecting data. Such a limited picture does not divulge "the whole of [the defendant's] physical movements," Carpenter, 138 S. Ct. at 2217, or track enough of his comings and goings so as to reveal "the privacies of life."

-

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

-

NOTE: BELOW IS FROM GANTS J. CONCURRENCE AND MUSINGS ON THE FUTURE OF ALPR. THE IDEA OF LEGAL PROCESS OPTIONS COMES FROM THIS SECTION.

GANTS, C.J. (concurring). I agree with the court that, if the State police had obtained historical locational data regarding the defendant's vehicle from enough automatic license plate readers (ALRPs) in enough locations, the mosaic that such collection would create of the defendant's movements "would invade a reasonable expectation of privacy and would constitute a search for constitutional purposes." Ante at 506. I also agree with the court that the locational information regarding the defendant that was obtained from four ALPRs at two fixed locations on two bridges falls short of creating the type of mosaic that would constitute a search within the meaning of either art. 14 of the Massachusetts Declaration of Rights or the Fourth Amendment to the United States Constitution. And I agree that the court is correct to forbear from declaring in this case "precisely how detailed a picture of the defendant's movements must be revealed to invoke constitutional protections."

-

For instance, if the State police maintain 1,000 ALPRs at different locations throughout the Commonwealth, it matters whether they searched for a suspect's vehicle from the data yielded by all 1,000 cameras or only by four cameras, and it matters whether they gathered this data for one day or one hundred days.

-

Pragmatically, I submit we
have two alternatives. Our first option is to determine based on the facts of a particular case when the locational mosaic of a targeted individual's movements crosses the threshold of the reasonable expectation of privacy. A mosaic above that threshold would require a search warrant based on probable cause, but a mosaic below that threshold would not require any court authorization.

-

This second alternative would mean that law enforcement agencies would need to obtain court authorization more often before retrieving targeted individual historical locational information in their possession because queries that would not require a showing of probable cause might still require a showing of reasonable suspicion. But the benefit to law enforcement would be that, if the police sought a court order based on reasonable suspicion and a reviewing court determined that the query sought locational data that could yield a mosaic of movement requiring a showing

of probable cause, the search would not be found unconstitutional (and the information collected would not be suppressed) if the reviewing court found that the affidavit supported a finding of probable cause. In contrast, where no court order was obtained and a reviewing court determined that probable cause or reasonable suspicion was required to support the retrieval of historical locational information, the data retrieved from the query would have to be suppressed even if law enforcement could have met the applicable standard.

-

[Note 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. We trust, however, that as our cases develop, this constitutional line gradually and appropriately will come into focus. "The judiciary risks error by elaborating too fully on the Fourth Amendment [or art. 14] implications of emerging technology before its role in society has become clear." Ontario v. Quon, 560 U.S. 746, 759 (2010).

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: Dan Mento
To: Pack, Noah (POL); Cyr, Mark (POL)
Cc: ddelucca@v2-global.com
Subject: Meeting Follow Up
Date: Monday, February 6, 2023 3:07:53 PM
Attachments: Falcon Long Range Overview (1).pdf
2023 Falcon Flex™ Overview .pdf
2023 Flock Overview for Law Enforcement (3).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 LTC Cyr and Sgt. Pack,

I appreciate the time you took to meet this morning. As we discussed and given the current challenges and limitations within the state regarding LPR, if you are interested in a limited project utilizing a few of our new Falcon Highway cameras as well as our Falcon Flex camera which can be moved around for special applications I believe it would be a good starting point. I have attached a few informational sheets on these camera systems. Please let me know if you have any questions.

I am happy to set up a camera mapping call with my Solutions Consultant who is former law enforcement and ran the LPR program at his department in GA which included Flock. We can work together to select an area and show you how we would recommend deploying our cameras in order to effectively cover that location. If you have some time in the next few weeks please let me know and we can schedule a follow up meeting to go over what a small scale deployment would look like.

I suspect that I did not fully answer each question that was brought up regarding how we effectively engage the communities that our cameras are in so we can get ahead of any concerns about how many cameras are deployed and where they are located. I am happy to also set up a call with our legal and external affairs teams here at Flock that handles these situations so we can dive into this deeper.

Feel free to give me a call on my cell phone if you have any questions. [redacted]

Thank you,

Dan

Dan Mento
Manager, Major Accounts (Eastern US)
914.350.6506 I Dan.mento@flocksafety.com

From: Jim Dowling
To: Pack, Noah (POL)
Subject: Motorola/NJ State Police ALPR Program
Date: Thursday, January 5, 2023 5:22:34 AM
Attachments: ag-Directive-2022-12_Updated-Directive-Regulating-Use-of-Automated-License-Plate-Recognition-(ALPR)-Technology.pdf
2022-0912_ARP-Automated-Licnese-Plate-Reader-Program-Administration-and-Guidelines.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 Noah, I was just provided the following information from my Motorola counterpart (Bob Duke) in NJ. I also included two attachments for your reference. Both individuals below are aware that you may be contacting them to discuss the NJ State Police ALPR program. My understanding is that deployment will start within the next 60 days after the formal PO is issued. Hope this information is useful.

https://www.njoag.gov/acting-ag-platkin-announces-availability-of-17-million-in-grants-to-reduce-gun-violence-and-combat-auto-theft-in-new-jersey/

The contact for the NJSP is:

Lt. Adam Pohlemus
Statewide ALPR Program
adam.polhemus@njsp.org
Cell: [redacted]

The state is deploying 400+ cameras throughout the state.

"Jim Sheehan is the NJ UASI leader. Much of the funding in NJ goes through UASI. Jim Sheehan is very good friends with the Colonel of the Massachusetts State Police."

James J Sheehan
Program Manager
Northern NJ-Newark/Jersey City UASI
30 King Road
Totowa, NJ 07512
(973) 837-7698 Office
[redacted] Cell
jsheehan@nnjuasi.org

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.
M. 513-292-0805
E. jdowling@motorolasolutions.com

Power Up Your Patrol! Get Started Today



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

From: Pack, Noah (POL)
To: Ryan, Kristin (POL)
Subject: MOU for LTC
Date: Saturday, May 6, 2023 3:32:47 PM
Attachments: DHS MOU Signature Sheet - chicopee PD.pdf
Chicopee MOU.pdf
TFL LPR MOUs 5-6-23 chicopee.pdf

Hi Kristin,

I may not make it to GHQ this week due to a trial starting in Springfield.

Could you please print this MOU request and add it to the folder for LTC Cyr to review?

Thank you very much,

Noah

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

From:	Cyr, Mark (POL)
To:	Kwon, Gina K. (EPS); Terrey, Susan (EPS)
Cc:	Mawn, John (POL); Pinkham, John (POL); Wheeler, Mark (POL); Diotte, Jeffrey (POL)
Subject:	MSP and DOT Equipment Collocation Request
Date:	Wednesday, July 5, 2023 2:39:24 PM
Attachments:	MSP DHS DOT Collocation Request 10-2022 Letterheard (8).doc MSP DHS DOT Collocation Request 7-23 Notes Update.doc

Good afternoon U/S Kwon and Terrey,
I have attached a letter that I sent to Joe Foti and Tony Wade (MA DOT) on October 26, 2022, requesting collocation of equipment, specifically ALPR cameras. In this letter, I highlighted the criticality of this equipment as it pertains to our public safety mission and detailed the nature of the request, the responsibilities the MSP would assume, and the anticipated sites for deployment of the cameras.

As discussed yesterday, Mr. Wade recently informed Sgt. Pack the DOT has not historically allowed MSP access to State resources, and this request would require a "policy change."

For a better understanding and to assist with the next steps, I have attached a Word document outlining a history of the request to include why this request benefits the Commonwealth. Unfortunately, in order to enable a "policy change," the next step in this request may have to be facilitated through respective Secretariats.

Please let me know if you have any questions/concerns.

Thank you!
Mark

Lieutenant Colonel Mark D. Cyr #2728
Massachusetts State Police
Division Commander
Division of Homeland Security and Preparedness
508-988-7301 (office)
G.L. c. 4 sec. 7 cl.26 (n)(security) *(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: Michael Roth
To: Pack, Noah (POL)
Subject: Neology MSP Updates 3/16
Date: Thursday, March 16, 2023 1:08:20 PM
Attachments: image001.png
image002.png
image003.png
MSP Status Report.pptx

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

Michael Roth
Application Development
Mobile: + [redacted]
Email: mroth@neology.net

13520 Evening Creek Dr E #460,
San Diego, CA 92128

www.neology.net

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

To: Toner, Kayla (OGR); Mboka-Boyer, Vicky (OGR)
Cc: Gray, Kellie (POL); Comeau, Melissa (POL)
Subject: POL - 6/30/23 Financial & Progress Report for Fusion Center and Critical Infrastructure Program FY20
Date: Monday, July 17, 2023 10:23:50 AM
Attachments: FSHSP20CFC Financial Report 6.30.23.pdf signed.pdf
FSHSP20CFC Progress Report 06.30.23.pdf
FUASI20CIP qtrly financial 6.30.23 zero report - signed.pdf

Hello Vicky and Kayla,

Please find attached Financial and Progress Report for the following programs below. Let us know if you might need anything else.

- FY20 Fusion Center/FSHSP20CFC
- FY20 Commonwealth Critical Infrastructure Program/FUASI20CIP

Thank you,

Jeff Ly
Accountant IV – Grants
Massachusetts State Police
470 Worcester Road
Framingham, MA 01712
508-988-7081
Jeff.Ly@pol.state.ma.us

From:	Ly, Jeff (POL)
To:	Toner, Kayla (OGR); Mboka-Boyer, Vicky (OGR)
Cc:	Gray, Kellie (POL); Comeau, Melissa (POL)
Subject:	POL - 6/30/23 Financial & Progress Report for Fusion Center and Critical Infrastructure Program FY20
Date:	Monday, July 17, 2023 10:24:00 AM
Attachments:	FSHSP20CFC Financial Report 6.30.23.pdf signed.pdf FSHSP20CFC Progress Report 06.30.23.pdf FUASI20CIP qtrly financial 6.30.23 zero report - signed.pdf FUASI20CIP Progress Report 06.30.23.pdf

---

Hello Vicky and Kayla,

Please find attached Financial and Progress Report for the following programs below. Let us know if you might need anything else.

- FY20 Fusion Center/FSHSP20CFC
- FY20 Commonwealth Critical Infrastructure Program/FUASI20CIP

Thank you,

Jeff Ly
Accountant IV – Grants
Massachusetts State Police
470 Worcester Road
Framingham, MA 01712
508-988-7081
Jeff.Ly@pol.state.ma.us

To: Mboka-Boyer, Vicky (OGR)
Cc: Rust, Rebecca (POL); Comeau, Melissa (POL)
Subject: POL - 9/30/23 Financial & Progress Report for Fusion Center and Critical Infrastructure Program
Date: Friday, October 13, 2023 11:57:40 AM
Attachments: FSHSP20CFC Quarterly Financial Report 9.30.23 signed.pdf
FUASI20CIP Quarterly Financial Report 9.30.23 signed.pdf
FSHSP21CFC Quarterly Financial Report 9.30.23 signed.pdf
FUASI21COM Quarterly Financial Report 9.30.23 signed.pdf
FSHSP22CFC Quarterly Financial Report 9.30.23 signed.pdf
FUASI22CIP Quarterly Financial Report 9.30.23 signed.pdf

Hi Vicky,

Please find attached Financial and Progress Report for the following programs below. Let us know if you might need anything else.

- FY20 Fusion Center/FSHSP20CFC
- FY20 Commonwealth Critical Infrastructure Program/FUASI20CIP
- FY21 Fusion Center/FSHSP21CFC/FUASI21CFC
- FY21 Continued Funding for Critical Infrastructure Program/FUASI21COM
- FY22 Fusion Center/FSHSP22CFC/FUASI22CFC
- FY22 Commonwealth Critical Infrastructure Program/FUASI22CIP

Thank you,

Jeff Ly
Accountant IV – Grants
Massachusetts State Police
470 Worcester Road
Framingham, MA 01712
508-988-7081
Jeff.Ly@pol.state.ma.us

From: Ly, Jeff (POL)
To: Mboka-Boyer, Vicky (OGR)
Cc: Rust, Rebecca (POL); Comeau, Melissa (POL)
Subject: POL - 9/30/23 Financial & Progress Report for Fusion Center and Critical Infrastructure Program
Date: Friday, October 13, 2023 11:59:06 AM
Attachments: FSHSP20CFC Quarterly Financial Report 9.30.23 signed.pdf
FUASI20CIP Quarterly Financial Report 9.30.23 signed.pdf
FSHSP21CFC Quarterly Financial Report 9.30.23 signed.pdf
FUASI21COM Quarterly Financial Report 9.30.23 signed.pdf
FSHSP22CFC Quarterly Financial Report 9.30.23 signed.pdf
FUASI22CIP Quarterly Financial Report 9.30.23 signed.pdf

Hi Vicky,

Happy Friday!
Please find attached Financial and Progress Report for the following programs below. Let us know if you might need anything else.

- FY20 Fusion Center/FSHSP20CFC
- FY20 Commonwealth Critical Infrastructure Program/FUASI20CIP
- FY21 Fusion Center/FSHSP21CFC/FUASI21CFC
- FY21 Continued Funding for Critical Infrastructure Program/FUASI21COM
- FY22 Fusion Center/FSHSP22CFC/FUASI22CFC
- FY22 Commonwealth Critical Infrastructure Program/FUASI22CIP

Thank you,

Jeff Ly
Accountant IV – Grants
Massachusetts State Police
470 Worcester Road
Framingham, MA 01712
508-988-7081
Jeff.Ly@pol.state.ma.us

From: EOTSS-Billing (MassIT)
To: Silva, Kyra (POL)
Cc: Small, Michelle (POL)
Subject: POL April 2023 Invoice
Date: Friday, May 26, 2023 9:01:37 AM
Attachments: POL Invoice - FY23 April.pdf
POL Pass-Through Statement - FY23 April.pdf
POL Charges - FY23 April.csv

Dear Kyra,

Attached is your April FY23 EOTSS Chargeback Invoice for POL.

April ITI's for EOTSS charges have been entered in MMARS. The Comptroller's policy requires that ITA's be processed for these charges within 30 days of issue.

Please ensure that your encumbrances (IE documents) for BCS, COR, PAS charges have sufficient funds encumbered for the remainder of the fiscal year. Per A&F notice, June 9th will be the deadline for new encumbrances or increases that total $75,000 or more. Our billing team can provide you a recent forecast of all IT Chargebacks for this fiscal year.

Also please contact the billing team (eotss-billing@mass.gov) to request an updated list of all approved BARS along with reviewing the attached Pass-through statement to ensure you have sufficient funds encumbered for all Pass-through charges.

Finally, as you process the ITA documents for BCS, COR, PAS charges please do not use any other object code other than U04 as these IT chargebacks should be coded to U04 object code as per the Comptroller's guidance. ITA documents for PAD charges should be coded as E05 object code.

If you have questions about these charges or require more detail, please email the billing team at EOTSS-Billing@mass.gov.

Sincerely,

The EOTSS Billing Team

From: EOTSS-Billing (MassIT)
To: Silva, Kyra (POL)
Cc: Small, Michelle (POL)
Subject: POL April 2023 Invoice
Date: Wednesday, May 31, 2023 11:17:39 AM
Attachments: POL Invoice - FY23 April.pdf
POL Pass-Through Statement - FY23 April.pdf
POL Charges - FY23 April.csv

Dear Kyra,

Attached is your April FY23 EOTSS Chargeback Invoice for POL.

April ITI's for EOTSS charges have been entered in MMARS. The Comptroller's policy requires that ITA's be processed for these charges within 30 days of issue.

The Pass-through statements sent last week with the April 2023 chargeback invoices had erroneous statuses for BARS. We have since corrected it and attached please find the updated pass-through statements with the correct status and please ignore previously sent Pass-through statement. Please contact EOTSS Billing Team (eotss-billing@mass.gov) if you have any questions.

Sincerely,

The EOTSS Billing Team

From: EOTSS-Billing (MassIT)
To: Silva, Kyra (POL)
Cc: Small, Michelle (POL)
Subject: POL August 2023 Invoice
Date: Thursday, October 19, 2023 12:13:40 PM
Attachments: POL Invoice - FY24 August.pdf
POL Pass-Through Statement - FY24 August.pdf
POL Charges - FY24 August.csv

Dear Kyra,

Attached is your August FY24 EOTSS Chargeback Invoice for POL.

Rate Changes

Office 365 G3 (full license) rate increased from $33.81/license/month in FY23 to $37.46/license/month in FY24.

Encumbrances and Payments

Please ensure that your encumbrances (IE documents) for BCS, COR, PAS charges have sufficient funds encumbered for the fiscal year. Our billing team can provide you a recent forecast of all IT Chargebacks for this fiscal year if you have not already received it.

Also please contact the billing team (eotss-billing@mass.gov) to request an updated list of all approved BARS along with reviewing the attached Pass-through statement to ensure you have sufficient funds encumbered for all Pass-through charges for the fiscal year.

As you process the ITA documents for BCS, COR, PAS charges please do not use any other object code other than U04 as these IT chargebacks should be coded to U04 object code as per the Comptroller's guidance.

If you have questions about these charges or require more detail, please email the billing team at EOTSS-Billing@mass.gov.

Sincerely,

The EOTSS Billing Team

From: EOTSS-Billing (MassIT)
To: Silva, Kyra (POL)
Cc: Small, Michelle (POL)
Subject: POL December 2022 Invoice
Date: Thursday, January 26, 2023 8:58:26 AM
Attachments: POL Invoice - FY23 December.pdf
POL Charges - FY23 December.csv
POL Pass-Through Statement - FY23 December.pdf

Dear Kyra,

Attached is your December FY23 EOTSS Chargeback Invoice for POL.

December ITI's for EOTSS charges have been entered in MMARS. The Comptroller's policy requires that ITA's be processed for these charges within 30 days of issue.

If you have questions about these charges or require more detail, please email the billing team at EOTSS-Billing@mass.gov.

Sincerely,

The EOTSS Billing Team

From: EOTSS-Billing (MassIT)
To: Silva, Kyra (POL)
Cc: Small, Michelle (POL)
Subject: POL February 2023 Invoice
Date: Wednesday, April 12, 2023 2:24:03 PM
Attachments: POL Invoice - FY23 February.pdf
POL Pass-Through Statement - FY23 February.pdf
POL Charges - FY23 February.csv

Dear Kyra,

Attached is your February FY23 EOTSS Chargeback Invoice for POL.

February ITI's for EOTSS charges have been entered in MMARS. The Comptroller's policy requires that ITA's be processed for these charges within 30 days of issue.

If you have questions about these charges or require more detail, please email the billing team at EOTSS-Billing@mass.gov.

Sincerely,

The EOTSS Billing Team

From: EOTSS-Billing (MassIT)
To: Silva, Kyra (POL)
Cc: Small, Michelle (POL)
Subject: POL January 2023 Invoice
Date: Wednesday, March 1, 2023 10:41:11 AM
Attachments: POL Invoice - FY23 January.pdf
POL Pass-Through Statement - FY23 January.pdf
POL Charges - FY23 January.csv

Dear Kyra,

Attached is your January FY23 EOTSS Chargeback Invoice for POL.

January ITI's for EOTSS charges have been entered in MMARS. The Comptroller's policy requires that ITA's be processed for these charges within 30 days of issue.

If you have questions about these charges or require more detail, please email the billing team at EOTSS-Billing@mass.gov.

Sincerely,

The EOTSS Billing Team

From: EOTSS-Billing (MassIT)
To: Silva, Kyra (POL)
Cc: Small, Michelle (POL)
Subject: POL January 2023 Invoice
Date: Friday, March 3, 2023 8:19:22 AM
Attachments: POL Invoice - FY23 January.pdf
POL Charges - FY23 January.csv
POL Pass-Through Statement - FY23 January.pdf

Dear Kyra,

Several customers have reported issues opening the attachments sent in our previous email. We apologize for any inconvenience and have attached new copies of the invoice.

Attached is your January FY23 EOTSS Chargeback Invoice for POL.

January ITI's for EOTSS charges have been entered in MMARS. The Comptroller's policy requires that ITA's be processed for these charges within 30 days of issue.

If you have questions about these charges or require more detail, please email the billing team at EOTSS-Billing@mass.gov.

Sincerely,

The EOTSS Billing Team

From: EOTSS-Billing (MassIT)
To: Silva, Kyra (POL)
Cc: Small, Michelle (POL)
Subject: POL July 2023 Invoice
Date: Monday, October 16, 2023 1:20:51 PM
Attachments: POL Invoice - FY24 July.pdf
POL Pass-Through Statement - FY24 July.pdf
POL Charges - FY24 July.csv

Dear Kyra,

Attached is your July FY24 EOTSS Chargeback Invoice for POL.

July 2023 ITI's for EOTSS charges have been entered in MMARS. The Comptroller's policy requires that ITA's be processed for these charges within 30 days of issue.

Rate Changes

Office 365 G3 (full license) rate increased from $33.81/license/month in FY23 to $37.46/license/month in FY24.

Encumbrances and Payments

Please ensure that your encumbrances (IE documents) for BCS, COR, PAS charges have sufficient funds encumbered for the fiscal year. Our billing team can provide you a recent forecast of all IT Chargebacks for this fiscal year if you have not already received it.

Also please contact the billing team (eotss-billing@mass.gov) to request an updated list of all approved BARS along with reviewing the attached Pass-through statement to ensure you have sufficient funds encumbered for all Pass-through charges for the fiscal year.

As you process the ITA documents for BCS, COR, PAS charges please do not use any other object code other than U04 as these IT chargebacks should be coded to U04 object code as per the Comptroller's guidance.

If you have questions about these charges or require more detail, please email the billing team at EOTSS-Billing@mass.gov.

Sincerely,

The EOTSS Billing Team

From: EOTSS-Billing (MassIT)
To: Silva, Kyra (POL)
Cc: Small, Michelle (POL)
Subject: POL June 2023 Invoice
Date: Friday, July 21, 2023 9:35:24 AM
Attachments: POL Invoice - FY23 June.pdf
POL Pass-Through Statement - FY23 June.pdf
POL Charges - FY23 June.csv

Dear Kyra,

Attached is your June FY23 EOTSS Chargeback Invoice for POL.

June ITI's for EOTSS charges have been entered in MMARS. The Comptroller's policy requires that ITA's be processed for these charges within 30 days of issue.

Please ensure that your encumbrances (IE documents) for BCS, COR, PAS charges have sufficient funds encumbered for the remainder of the fiscal year. Our billing team can provide you a recent forecast of all IT Chargebacks for this fiscal year.

Also please contact the billing team (eotss-billing@mass.gov) to request an updated list of all approved BARS along with reviewing the attached Pass-through statement to ensure you have sufficient funds encumbered for all Pass-through charges for the remainder of the fiscal year.

As you process the ITA documents for BCS, COR, PAS charges please do not use any other object code other than U04 as these IT chargebacks should be coded to U04 object code as per the Comptroller's guidance. ITA documents for PAD charges should be coded as E05 object code.

Finally, we are getting ready for the next fiscal year and we will be sharing IT chargeback forecasts for BCS and COR charges for FY 2024 during mid-August which can be used to support your initial IE amounts. We do not forecast for PAS charges as these are pass-through charges so it will not be part of the FY 2024 forecast.

Sincerely,

The EOTSS Billing Team

From: EOTSS-Billing (MassIT)
To: Silva, Kyra (POL)
Cc: Small, Michelle (POL)
Subject: POL March 2023 Invoice
Date: Monday, May 8, 2023 3:43:11 PM
Attachments: POL Invoice - FY23 March.pdf
POL Pass-Through Statement - FY23 March.pdf
POL Charges - FY23 March.csv

Dear Kyra,

Attached is your March FY23 EOTSS Chargeback Invoice for POL.

March ITI's for EOTSS charges have been entered in MMARS. The Comptroller's policy requires that ITA's be processed for these charges within 30 days of issue.

If you have questions about these charges or require more detail, please email the billing team at EOTSS-Billing@mass.gov.

Sincerely,

The EOTSS Billing Team

From: EOTSS-Billing (MassIT)
To: Silva, Kyra (POL)
Cc: Small, Michelle (POL)
Subject: POL May 2023 Invoice
Date: Wednesday, June 21, 2023 2:10:14 PM
Attachments: POL Invoice - FY23 May.pdf
POL Pass-Through Statement - FY23 May.pdf
POL Charges - FY23 May.csv

Dear Kyra,

Attached is your May FY23 EOTSS Chargeback Invoice for POL.

May ITI's for EOTSS charges have been entered in MMARS. The Comptroller's policy requires that ITA's be processed for these charges within 30 days of issue.

Please ensure that your encumbrances (IE documents) for BCS, COR, PAS charges have sufficient funds encumbered for the remainder of the fiscal year. Our billing team can provide you a recent forecast of all IT Chargebacks for this fiscal year.

Also please contact the billing team (eotss-billing@mass.gov) to request an updated list of all approved BARS along with reviewing the attached Pass-through statement to ensure you have sufficient funds encumbered for all Pass-through charges for the remainder of the fiscal year.

As you process the ITA documents for BCS, COR, PAS charges please do not use any other object code other than U04 as these IT chargebacks should be coded to U04 object code as per the Comptroller's guidance. ITA documents for PAD charges should be coded as E05 object code.

Finally, we are getting ready for the next fiscal year and we will be sharing IT chargeback forecasts for BCS and COR charges for FY 2024 during mid-August which can be used to support your initial IE amounts. We do not forecast for PAS charges as these are pass-through charges so it will not be part of the FY 2024 forecast.

Sincerely,

The EOTSS Billing Team

From: EOTSS-Billing (MassIT)
To: Silva, Kyra (POL)
Cc: Small, Michelle (POL)
Subject: POL November 2022 Invoice
Date: Thursday, January 12, 2023 8:49:37 AM
Attachments: POL Invoice - FY23 November.pdf
POL Charges - FY23 November.csv
POL Pass-Through Statement - FY23 November.pdf

Dear Kyra,

Attached is your November FY23 EOTSS Chargeback Invoice for POL.

November ITI's for EOTSS charges have been entered in MMARS. The Comptroller's policy requires that ITA's be processed for these charges within 30 days of issue.

If you have questions about these charges or require more detail, please email the billing team at EOTSS-Billing@mass.gov.

Sincerely,

The EOTSS Billing Team

From: Scott, Michael (POL)
To: Hean, Steven (POL); Perry, Jeffrey (POL); OToole, Kevin (POL); DeCaro, Michael (POL)
Subject: Policy and Rules and Regs
Date: Wednesday, August 30, 2023 10:49:31 AM
Attachments: All Policy-Rules-Regs AO 08-30-23.pdf
image001.png

Respectfully,

Dlt. Michael E. Scott #3508

Detective Lieutenant Michael E. Scott #3508
Massachusetts State Police
Division of Standards and Training - Office of Professional Integrity and Accountability
470 Worcester Road
Framingham, Massachusetts 01702

From: Mason, Michelle (POL)
To: Dwyer, Kevin (POL); Sweeney, Jeremy (POL)
Subject: Policy and Rules
Date: Wednesday, October 25, 2023 11:09:00 AM
Attachments: P&P Combined 10-13-23.pdf
Outlook-0lvhmkvb.png

From a friend of mine, he combined all of them as of the most recent updates. I also have R&R which he didn't combine but are up to date. I'll send those under separate email.

Share them with the people in the inner circle only!

MAM

Detective Lieutenant Michelle A. Mason #2892
Massachusetts State Police
Office of Professional Integrity and Accountability
470 Worcester Road
Framingham, MA 01702
Phone #: (508) 988-7001
Cell #: [redacted] M.G.L. c. 4.sec. 7.cl.26 (n)(security)
Fax #: (508) 820-2185

From: Pack, Noah (POL)
To: Cyr, Mark (POL)
Subject: Policy Draft Notes
Date: Monday, March 13, 2023 10:01:03 AM
Attachments: ALPR Policy Change Highlights 3-13-23.docx

LTC: a summary of some of the proposed changes in the policy draft that deal with privacy considerations.

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: Brunelli, Daniel (POL); Staples, Jennifer (POL)
Cc: Cyr, Mark (POL)
Subject: Policy Draft Notes
Date: Monday, March 13, 2023 10:48:59 AM
Attachments: ALPR Policy Change Highlights 3-13-23.docx
TRF-11 Automatic License Plate Recognition DRAFT 19 3-13-23.docx

---

Good morning Jenn:

Attached is a short summary of some of the policy changes that we discussed. I have also added highlights to the policy draft itself for your review. There are additional changes in wording or organization of the document that I did not highlight, as this is intended to note the specific changes that deal with privacy & best practices. Please let me know if I can provide anything further.

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: Condlin, Christopher (POL)
To: Powers, Liam (POL)
Subject: Policy Request
Date: Tuesday, April 18, 2023 9:33:03 AM
Attachments: ADM-47 Bias-Based Policing.pdf
TRF-01 Mission Goals and Objectives New 11-05-08.pdf
TRF-02 Patrol Revised Renumbered 4-23-09.pdf
TRF-03 Selective Traffic Enforcement Revised Renumber 11-05-08.pdf
TRF-04 Motor Vehicle Pursuits 5-10-2012.pdf
TRF-04A Foot Pursuits New 4-23-09.pdf
TRF-05 Traffic Incident Management New 11-05-08.pdf
TRF-07 Motor Vehicle Stops Revised 11-05-08.pdf
TRF-08 Citations Revised 4-23-09.pdf
TRF-09 Towing Revised 6-14-2018.pdf
TRF-10 Vehicle Inventory Revised 4-23-09.pdf
TRF-11 Automatic License Plate Recognition Revised 10-1-2019 with highlights.pdf
TRF-12 Crash Investigations Revised 4-23-09.pdf
TRF-14 OUI Alcohol Revised 7-22-2014.pdf
TRF-14B Preliminary Portable Breath Test Devices 7-22-2014.pdf
TRF-15 Sobriety Checkpoints Revised 4-23-09.pdf
TRF-16 Speed Measuring Devices 4-23-09.pdf
TRF-17 Emergency Roadblocks Revised 4-23-09.pdf
TRF-20 Department Vehicle Crash Revised 7-8-09.pdf
TRF-21 Tire Deflat Revised 4-23-09.pdf
TRF-22 Escorts and Relays revised 5.21.2018.pdf

Legal has received a court order to produce the following documents related to Trooper Ali Jaafar #4532 in effect on 12/24/2020 who was assigned to D-4 at the time. At your earliest convenience, could you please forward a copy to me.

1. MSP general policy regarding motor vehicle stops and tows
2. MSP general order ADM-47 entitled “Biased Based Policing”
3. MSP policy entitled “Duties of Patrol”
4. Policies and procedures pertaining to Trooper Ali Jaafar’s unit
5. the policy/manual for officers in Division of field services

Sgt. Christopher Condlin #2970
Strategic Planning and Analysis Section
Office of the Superintendent
617-963-4295

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: Condlin, Christopher (POL)
To: Pinkes, William (POL)
Subject: Policy Revision
Date: Tuesday, May 30, 2023 12:56:00 PM
Attachments: TRF-11 Automatic License Plate Recognition DRAFT 2023 (1) (1).docx

---

Sir,

When you have a minute, would you please take a look at the attached policy. This is likely to be pushed out ASAP.

Thank you,
Chris

Sgt. Christopher Condlin #2970
Strategic Planning and Analysis Section
Office of the Superintendent
508-988-7439

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)
To: Matthew Post
Subject: Policy
Date: Thursday, May 4, 2023 4:35:13 PM
Attachments: TRF-11 Nov21.pdf

Matt, attached is our current policy.

Respectfully,

Noah

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

From: Fafard, Matthew (POL)
To: Demers, Joseph (CHS)
Subject: Policy
Date: Tuesday, August 22, 2023 12:01:10 PM
Attachments: Massachusetts CJIS User Agreement 8-10-23.pdf
Global Justice and PS Info Sharing Policy 8-10-23.pdf
TRF-11 Automatic License Plate Recognition.docx
Acceptable Use Policy.zip
Misuse Schedule.pdf
Physical Security.zip

Captain Matthew R. Fafard
Massachusetts State Police
Division of Administrative Services
470 Worcester Road, Framingham, MA 01702
Office: 508-820-2107
matthew.fafard@pol.state.ma.us

From: Procopio, David (POL)
To: Driscoll, Elaine (EPS)
Subject: Proposed statement/background + policy
Date: Friday, October 20, 2023 10:18:00 AM
Attachments: image001.png
TRF-11.pdf

Here is a proposed statement and two background points, plus the policy. I don't have any answers yet on numbers of times used.

Statement:
"The ability to query information about vehicles connected to serious crimes, through both the MSP's automated license plate readers and the DOT's tolling gantries, is a valuable tool to assist in capturing dangerous offenders, securing justice for their victims, and protecting public safety and homeland security. The MSP utilizes both systems judiciously and in accordance with state and federal laws and Constitutional rights of individuals."
-Me

Background:
-Use of the MSP's ALPR system is governed by a rigorous Departmental policy, TRF-11 (copy attached to this response).
-MSP investigators do not have direct access to the DOT gantry information, and request such data from the DOT's legal division via a thorough process that ensures all relevant criteria and safeguards are met.

Dave Procopio
Director, Media Relations Unit
Massachusetts State Police

To: Driscoll, Elaine (EPS)
Subject: Proposed statement/background + policy
Date: Friday, October 20, 2023 10:18:25 AM
Attachments: image001.png
TRF-11.pdf

Here is a proposed statement and two background points, plus the policy. I don't have any answers yet on numbers of times used.

Statement:
The ability to query information about vehicles connected to serious crimes, through both the MSP's automated license plate readers and the DOT's tolling gantries, is a valuable tool to assist in capturing dangerous offenders, securing justice for their victims, and protecting public safety and homeland security. The MSP utilizes both systems judiciously and in accordance with state and federal laws and Constitutional rights of individuals.
-Me

Background:
-Use of the MSP's ALPR system is governed by a rigorous Departmental policy, TRF-11 (copy attached to this response).
-MSP investigators do not have direct access to the DOT gantry information, and request such data from the DOT's legal division via a thorough process that ensures all relevant criteria and safeguards are met.

Dave Procopio
Director, Media Relations Unit
Massachusetts State Police

From: AmtrakIntelTeam
Subject: Rail Watch for the week ending 20 November
Date: Monday, November 20, 2023 9:54:57 AM
Attachments: Rail Watch_November_20_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.

Please find attached Rail Watch for the week ending 20 November.

Thank You,

Amtrak Police Department
Office of Intelligence and Analysis
AmtrakIntelTeam@amtrak.com
Report Suspicious Activity to 800-331-0008

From: Rambo, Glenn
Subject: Rail Watch for the week ending 20 November
Date: Monday, November 20, 2023 10:05:52 AM
Attachments: Rail Watch November 20 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.

Good morning and Happy Thanksgiving Week. Please see the attached Amtrak Police Intelligence Unit Rail Watch Weekly and share with your Law Enforcement and Public Safety partners.

Have a great week and Happy Thanksgiving from Amtrak Police Office of Intelligence and Analysis!!

Detective Glenn Rambo #213
Amtrak Police Department
Office of Intelligence and Analysis
VIP & Dignitary Move Coordinator
Nationwide Fusion Center Liaison
Field Intelligence Officer Coordinator
900 2nd Street N.E. Suite #300
Washington DC 20002
[redacted] **Cell**
1-800-331-0008 (24/7 APD Radio Room)

From: Michael Roth
To: Pack, Noah (POL)
Cc: Kory Koster; John Tedona; Luke Normington; ALPR_Support
Subject: Random GPS problem Update. [ref:_00D1N1wyfS._5003I1SdbtP:ref]
Date: Wednesday, January 25, 2023 1:35:20 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.

Noah, I wanted to touch base and let you know that with Kory's help we were able to access CR.1772 and gather data on the GPS issues, were reviewing the logs. In the meantime I update that units to PAGIS version 2.15.2.11 that should resolve those hotlist issues and a few others. But lets keep a eye on his data and see if he still gets random GPS in the meantime, that system was pretty consistently showing bad GPS. We also have a fix for the B/W images with color ocr capture, I did not apply that fix to CR.1772 as I just received and its not been tested thoroughly yet. Will touch base in our meeting to discuss plans to update your mobiles.

Michael Roth
Application Development
Mobile: + [redacted]
Email: mroth@neology.net

13520 Evening Creek Dr E #460,
San Diego, CA 92128

www.neology.net

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

From: Pack, Noah (POL)
To: Gaffney, Christopher
Subject: Re: [EXTERNAL] - Re: BOSS Login/password
Date: Wednesday, March 15, 2023 2:36:54 PM
Attachments: image002.png
ALPR TENANT MOU 2023.docx
Outlook-j43egagz.png

Chris,

Please have a representative from your Department sign this MOU. I will explain further on the phone in a few minutes.

Respectfully,

Noah

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

From: Gaffney, Christopher <cgaffney@danversma.gov>
Sent: Tuesday, March 14, 2023 3:37 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: RE: [EXTERNAL] - Re: BOSS Login/password

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

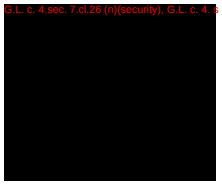
[redacted] – I am just leaving for the day. Are you available tomorrow?

Detective Christopher Gaffney
Criminal Investivation Division
Office : 978-774-1388 ext. 5
Fax : 978-777-0268
Email : cgaffney@danversma.gov
https://danverspolice.com/

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Sent: Tuesday, March 14, 2023 3:37 PM

To: Gaffney, Christopher <cgaffney@danversma.gov>
Subject: Re: [EXTERNAL] - Re: BOSS Login/password

Got it. What's your cell phone number?

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


From: Gaffney, Christopher <cgaffney@danversma.gov>
Sent: Tuesday, March 14, 2023 2:59 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Re: [EXTERNAL] - Re: BOSS Login/password

CAUTION: This email originated from a sender outside of the 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 the login I was referring to

Detective Christopher Gaffney
Criminal Investigation Division
Danvers Police Department
120 Ash Street
Danvers, MA 01923
Office: 978-774-1388
Fax: 978-777-0268
Email: cgaffney@danversma.gov

From: Gaffney, Christopher
Sent: Tuesday, March 14, 2023 2:52:47 PM
To: Pack, Noah (POL) <noah.pack@state.ma.us>
Subject: Re: [EXTERNAL] - Re: BOSS Login/password

Roger, could we set up a time to update our LPR server. I never connected with you in the past.

I'm handing this collateral over to a new officer soon and need to get everything squared away.

Thank you,

Detective Chris Gaffney
Criminal Investigation Division
Danvers Police Department
120 Ash Street
Danvers, MA 01923
(Office) 978-774-1388 ext. 5
(Cell) [redacted]

On Mar 14, 2023, at 2:49 PM, Pack, Noah (POL) <noah.pack@state.ma.us> wrote:

Hi Chris,

The login/password credentials should give access to the mobile processor system, but not to the boss software, as I believe you are indicating. At this time, all searches and hotlist requests should go through the Commonwealth Watch Center at fusion@pol.state.ma.us. We are working with the vendor to develop a mechanism to allow external users to search their contributed data, but it's not yet in place in the new software. If I misinterpreted your request that you were referring to something else, please let me know.

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: Gaffney, Christopher <cgaffney@danversma.gov>
Sent: Tuesday, March 14, 2023 2:44:20 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Williamson, Timothy <twilliamson@danversma.gov>
Subject: BOSS Login/password

CAUTION: This email originated from a sender outside of the 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 Sgt.,

I left you a voicemail regarding our previous attempts to update our server. I now realize I don't have my login or password for the BOSS server itself. Brian Egnitz said this would be something you could assist with as well.

Respectfully,

Chris Gaffney

Detective Christopher Gaffney
Criminal Investigation Division
Danvers Police Department
120 Ash Street
Danvers, MA 01923
Office: 978-774-1388
Fax: 978-777-0268
Email: cgaffney@danversma.gov

From: Pack, Noah (POL)
To: Gaffney, Christopher
Subject: Re: [EXTERNAL] - Re: BOSS Login/password
Date: Friday, March 17, 2023 8:57:29 AM
Attachments: image002.png
TRF-11 Nov21.pdf

Good morning Chris,

The company responded yesterday night that they allowed the IP address we gave them. I don't yet see your device in the system. Please have someone turn it on today so it tries to connect. Let me know when that has been done and I'll check again.

Please note that Danvers PD will be responsible (per the MOU) for selecting and training personnel to use this system. The MOU requires that the provisions of our policy be observed, and I have attached the most recent version. Please let me know if you have any questions.

One important guideline is that an LPR hit/alert alone should not be used as RS/PC to stop a car or take enforcement action. In the event of a misread or a match to a different state, the officer must "weed" these out before taking action. A best practice is to do the following:

Prior to initiation of a stop or enforcement action based upon an ALPR hit or alert, confirm the hit or alert, to include:

- *Verify the plate:* Visually verify that the vehicle plate matches the ALPR system's 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 that generated the hit/alert (e.g., is the vehicle still stolen), through:
    - Criminal Justice Information System (CJIS);
    - National Crime Information Center (NCIC);
    - Department's Records Management System (RMS); or
    - Another appropriate source of data

Similarly, documentation of an enforcement action after an LPR hit or alert should generally not indicate the hit or alert was the reason for the stop. If done correctly, it was not. The alert drew the officer's attention to the situation and vehicle, but the officer's direct observations and verification of the alert (i.e., a live CJIS query showing the vehicle was confirmed to be stolen) should provide the RS/PC. I am not suggesting to leave the LPR out of the report, of course, but to understand that it should be corroborated before taking action.

Respectfully,

Noah

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

From: Gaffney, Christopher <cgaffney@danversma.gov>
Sent: Friday, March 17, 2023 8:09 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Williamson, Timothy <twilliamson@danversma.gov>
Subject: RE: [EXTERNAL] - Re: BOSS Login/password

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

Good morning Sgt.,

I was off yesterday and wanted to follow up today and see about that three step process the MSP follows before stopping a vehicle based on the LPR hit. Also, is the system fully functional?

Respectfully,

Detective Christopher Gaffney
Criminal Investivation Division
Office : 978-774-1388 ext. 5
Fax : 978-777-0268
Email : cgaffney@danversma.gov
https://danverspolice.com/

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Sent: Wednesday, March 15, 2023 2:37 PM
To: Gaffney, Christopher <cgaffney@danversma.gov>
Subject: Re: [EXTERNAL] - Re: BOSS Login/password

Chris,

Please have a representative from your Department sign this MOU. I will explain further on the phone in a few minutes.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Homeland Security and Preparedness
[redacted]vision Commander

From: Gaffney, Christopher <cgaffney@danversma.gov>
Sent: Tuesday, March 14, 2023 3:37 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: RE: [EXTERNAL] - Re: BOSS Login/password

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

978-880-3115 – I am just leaving for the day. Are you available tomorrow?

Detective Christopher Gaffney
Criminal Investivation Division
Office : 978-774-1388 ext. 5
Fax : 978-777-0268
Email : cgaffney@danversma.gov
https://danverspolice.com/

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Sent: Tuesday, March 14, 2023 3:37 PM
To: Gaffney, Christopher <cgaffney@danversma.gov>
Subject: Re: [EXTERNAL] - Re: BOSS Login/password

Got it. What's your cell phone number?

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

[redacted]

From: Gaffney, Christopher <cgaffney@danversma.gov>
Sent: Tuesday, March 14, 2023 2:59 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Re: [EXTERNAL] - Re: BOSS Login/password

CAUTION: This email originated from a sender outside of the 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 the login I was referring to

Detective Christopher Gaffney
Criminal Investigation Division
Danvers Police Department
120 Ash Street
Danvers, MA 01923
Office: 978-774-1388
Fax: 978-777-0268
Email: cgaffney@danversma.gov

From: Gaffney, Christopher
Sent: Tuesday, March 14, 2023 2:52:47 PM
To: Pack, Noah (POL) <noah.pack@state.ma.us>
Subject: Re: [EXTERNAL] - Re: BOSS Login/password

Roger, could we set up a time to update our LPR server. I never connected with you in the past.

I'm handing this collateral over to a new officer soon and need to get everything squared away.

Thank you,

Detective Chris Gaffney
Criminal Investigation Division
Danvers Police Department
120 Ash Street
Danvers, MA 01923
(Office) 978-774-1388 ext. 5
(Cell) [redacted]

On Mar 14, 2023, at 2:49 PM, Pack, Noah (POL) <noah.pack@state.ma.us> wrote:

Hi Chris,

The login/password credentials should give access to the mobile processor system, but not to the boss software, as I believe you are indicating. At this time, all searches and hotlist requests should go through the Commonwealth Watch Center at fusion@pol.state.ma.us. We are working with the vendor to develop a mechanism to allow external users to search their contributed data, but it's not yet in place in the new software. If I misinterpreted your request that you were referring to something else, please let me know.

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: Gaffney, Christopher <cgaffney@danversma.gov>
Sent: Tuesday, March 14, 2023 2:44:20 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Williamson, Timothy <twilliamson@danversma.gov>
Subject: BOSS Login/password

CAUTION: This email originated from a sender outside of the 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 Sgt.,

I left you a voicemail regarding our previous attempts to update our server. I now realize I don't have my login or password for the BOSS server itself. Brian Egnitz said this would be something you could assist with as well.

Respectfully,

Chris Gaffney

Detective Christopher Gaffney
Criminal Investigation Division

Danvers Police Department
120 Ash Street
Danvers, MA 01923
Office: 978-774-1388
Fax: 978-777-0268
Email: cgaffney@danversma.gov

From: Pack, Noah (POL)
To: Breck, Kathy
Cc: Martucci, J; Schwarz, William J
Subject: Re: [External] FW: SPD and ALPR MOU TM 22-12660
Date: Wednesday, April 12, 2023 2:55:15 PM
Attachments: ALPR TENANT MOU SPD 4-23.docx

Good afternoon Kathy,

Hope you are enjoying this early start to summer! I'm reaching out to touch base on finalizing the ALPR MOU between MSP and Springfield. I've attached what I understand is the latest version of this document with Springfield's requested changes and the name of our new agency head.

Could you kindly review and assist me with getting this executed?

Thank you,

Noah

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

From: Breck, Kathy <KBreck@springfieldcityhall.com>
Sent: Monday, October 24, 2022 11:35 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Martucci, J <jmartucci@springfieldpolice.net>; Schwarz, William J <WSchwarz@springfieldpolice.net>; Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>
Subject: RE: [External] FW: SPD and ALPR MOU TM 22-12660

CAUTION: This email originated from a sender outside of the 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 Sgt. Pack.
I forwarded your 9/12/22 email to Bill Schwarz at SPD this morning for his review. Sorry for the delay on the response. Thank you.
Kathy Breck 10/24/22

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: Pack, Noah (POL) <noah.pack@state.ma.us>
Sent: Monday, September 12, 2022 1:52 PM
To: Breck, Kathy <KBreck@springfieldcityhall.com>
Cc: Martucci, J <jmartucci@springfieldpolice.net>; Schwarz, William J <WSchwarz@springfieldpolice.net>; Staples, Jennifer (POL) <jennifer.staples2@state.ma.us>
Subject: [External] FW: SPD and ALPR MOU

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
CAUTION: This email originated outside our organization; please use caution.

From: Greg Demeter
To: Quinn, Dermot (POL)
Subject: RE: ALPR Directive
Date: Wednesday, February 15, 2023 5:49:00 PM
Attachments: ag-Directive-2022-12_Updated-Directive-Regulating-Use-of-Automated-License-Plate-Recognition-(ALPR)-Technology.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.

Sorry about that. This is the new one, much more relevant than the first one I sent, updated to more modern standards.

From: Quinn, Dermot (POL) <dermot.quinn@state.ma.us>
Sent: Wednesday, February 15, 2023 4:51 PM
To: Greg Demeter <gdemeter@nnjuasi.org>; James Sheehan <jsheehan@nnjuasi.org>
Subject: RE: ALPR Directive

Hi Greg,

Just finished reading the policy you sent. Nicely done and contains a lot of material I think I can use to convince people that we don't need to reinvent the wheel up here.

The first document you attached dealt with "pandemic" issues. Could it be the wrong document? I also noticed the Policy had the five year retention language, and I recalled that you had mentioned it was changed to three.

Thanks again for sending the information my way.

Dermot

Dermot J. Quinn #1765
Criminal Information Section
Division of Homeland Security
Massachusetts State Police
617 590-1450
dermot.quinn@pol.state.ma.us
(Ret Lt Col MSP)

From: Greg Demeter <gdemeter@nnjuasi.org>
Sent: Tuesday, February 14, 2023 12:41 PM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; James Sheehan <jsheehan@nnjuasi.org>
Subject: RE: ALPR Directive

CAUTION: This email originated from a sender outside of the 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 believe we did meet at that ALPR meeting. When you get a chance, propose some days and times that you can talk and we will get on a phone call to discuss ALPR. Stay safe in the meantime.

Greg

From: Quinn, Dermot (POL) <dermot.quinn@state.ma.us>
Sent: Tuesday, February 14, 2023 12:31 PM
To: Greg Demeter <gdemeter@nnjuasi.org>; James Sheehan <jsheehan@nnjuasi.org>
Subject: RE: ALPR Directive

Hi Greg,

Thanks for the quick response. It is very much appreciated. I can't remember if we met before. I am friendly with several of the NJ team (Colonel Callahan,

Geoff Noble, Ray Guidetti, Joe Brennan, etc). We attended an ALPR meeting sponsored by NJSP and NYPD a few years back and I might have met you there.

I used to tell anyone who would listen that ALPR was our best bang for our technology buck that I had seen in a long time. We had a great opportunity to get it right, but like the "old" Red Sox, we constantly let the ball go between our legs.

When I was running DIS and DHS, I stressed out a lot about ALPR and I have some things that I'll discuss with you when we can talk. That being said, I was never able to get the state to take full advantage of this game changing technology. Ironically, being a man who rarely has an original idea, a lot of our program was based on what we learned in New Jersey and New York (I'll deny the New York part if questioned outside this group).

Now that I am retired and happily working in obscurity in a small office at a non-General Headquarters site, I want to take one more run at trying to point our state policy people in the right direction. Undoubtedly your input, along with Father James Sheehan from St.

Patrick's, will help put us on the right path.

All the best,

Dermot

From: Greg Demeter <gdemeter@nnjuasi.org>
Sent: Monday, February 13, 2023 4:56 PM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; James Sheehan <jsheehan@nnjuasi.org>
Subject: RE: ALPR Directive

CAUTION: This email originated from a sender outside of the 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,

Attached you will find the ALPR directive which we updated (yes, I had to work directly with Sheehan on this for several weeks, in case you were wondering) in late 2022 and it was made effective January 2023. What we submitted to the AG's office was quite a bit longer and certainly more in depth, but the Deputy AG we worked with did a pretty good job of cutting it down as he wanted to keep it under 10 pages. There are some holes in the policy as a result, that we've been realizing over the past month, but overall it is a pretty good document. Also attached is our 2010 directive that was in effect until January of this year.

The state of play in New Jersey was not wholly unlike what you describe in Mass, but what the AG's office did for us is create a state ALPR coordinator who has the ability to make rules and run the whole program. Any law enforcement agency who uses ALPRs, either by deploying them or using the data, has to follow the directive, which also means following the state coordinator. Vendors who provide ALPR for law enforcement agencies in NJ must share their data into a central depository, among other things. We are attempting to create one place to search all ALPR reads in the state. This is still being built, and it is slow and painful, but we are going in the right direction for sure.

I would be happy to speak with you if you have further questions. I ran the NJSP ALPR program for about 6 years prior to my retirement in Jan 2021, and they have me back helping out a little bit now so I can answer most questions.

Thanks,

Greg

From: Quinn, Dermot (POL) <dermot.quinn@state.ma.us>
Sent: Monday, February 13, 2023 4:38 PM
To: James Sheehan <jsheehan@nnjuasi.org>; Greg Demeter <gdemeter@nnjuasi.org>
Subject: RE: ALPR Directive

Ok Jim thanks.

My meeting is next Tuesday with our Executive Office of Public Safety. As usual in Massachusetts, the state has not provided guidance as far as LPR is concerned and we find ourselves exactly where we didn't want to be. The private sector is dealing directly with the cities and towns while state agencies struggle to get a clear direction as to what our policy is. We now have at least four different LPR systems and no single database.

Greg, anything you can provide would be helpful.

Thanks,

Dermot

Dermot J. Quinn #1765
Criminal Information Section
Division of Homeland Security
Massachusetts State Police
617 590-1450
dermot.quinn@pol.state.ma.us
(Ret Lt Col MSP)

From: James Sheehan <jsheehan@nnjuasi.org>
Sent: Monday, February 13, 2023 12:31 PM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Greg Demeter <gdemeter@nnjuasi.org>
Subject: ALPR Directive

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

Dermot,
Greg Demeter is retired from NJSP and is working with both the UASI and the SP on the statewide ALPR project. He will get you the updated AG Directive and can answer any questions on our project.

Jim

James J Sheehan
Program Manager
Northern NJ-Newark/Jersey City UASI
30 King Road
Totowa, NJ 07512
(973) 837-7698 Office
[redacted] Cell

The information contained in this transmission is for the sole use of the intended recipient(s) and may contain confidential and privileged information and may be considered advisory, consultive and deliberative material under OPRA.
Any unauthorized review; use, disclosure or distribution of this communication is strictly prohibited. If you have received this e-mail in error, please contact the sender by reply e-mail and destroy all paper and electronic copies of the original message

From: Eric Watson
To: Mathew Post; Pack, Noah (POL)
Subject: Re: ALPR MOU
Date: Friday, May 5, 2023 7:47:30 AM
Attachments: ALPR MOU.pdf

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

Hi Noah, Signed MOU attached. Thanks, Eric

On Mon, May 1, 2023 at 11:27 AM Mathew Post <mpost@chicopeepolice.com> wrote:

> MOU for neology
>
> **Sergeant Mathew Post**
> Chicopee Police Department
> 110 Church Street
> Chicopee, MA 01020
> Phone: 413-594-1743
>
> The preceding email message (including any attachments) contains information that may be confidential, may be protected by 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.
>
> ---------- Forwarded message ---------
> From: **Pack, Noah (POL)** <noah.pack@state.ma.us>
> Date: Mon, May 1, 2023 at 11:26 AM
> Subject: ALPR MOU
> To: Matthew Post <mpost@chicopeepolice.com>
>
> **Sergeant Noah H. Pack**
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> Office of the Division Commander

--
Deputy Chief Eric Watson
Chicopee, MA Police Dept.
Research & Development

413-377-4028



From: Pack, Noah (POL)
To: Pinkes, William (POL)
Cc: Walczak, Ryan (POL)
Subject: Re: ALPR Operator Training
Date: Tuesday, August 8, 2023 1:25:14 PM
Attachments: image001.png

DLt. Pinkes,

That is a different area than the cruiser mounted LPRs, which is the reason I inquired as the definition of an LPR operator in an earlier email. Is there a separate standard we should be considering related to that inquiry?

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

From: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Sent: Tuesday, August 8, 2023 1:11 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Walczak, Ryan (POL) <ryan.walczak@pol.state.ma.us>
Subject: RE: ALPR Operator Training

Good afternoon,

Thank you for assisting me with this information. Recognizing that we are utilizing very limited numbers of cruiser mounted ALPR's, I would pose the same questions to ascertain compliance with stationary ALPR systems.

Could you advise the who/what/when related to training for the stationary systems.

Thank you in advance for your assistance gathering this information. Don't hesitate to reach out directly with any questions/concerns either of you may have. I appreciate your help.

V/R,
Bill P.

Bill Pinkes
Accreditation Manager
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-808-3448

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Monday, August 7, 2023 3:47 PM
To: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Cc: Walczak, Ryan (POL) <ryan.walczak@pol.state.ma.us>
Subject: Re: ALPR Operator Training

DLt. Pinkes,

Apologies for the delays; I have had limited time at work over the past few weeks.

The Department currently has very few cruiser ALPRs in service. Attached is a record of those who are currently operating a cruiser with a functional and connected ALPR system and their associated training dates. The majority of the Department's cruiser mounted ALPR systems are not currently in service, and those cruisers/users are not reflected on this list. When and if those systems are brought online and placed into service, we will continue to ensure that the users are trained and our documentation is updated.

In past years, training has been done at times by both the systems' vendor (Neology) and our staff. Our user training currently includes, at a minimum, a familiarization on how to use the system, review of our policy with emphasis on the areas that apply to cruiser LPRS, such as hit confirmation procedures/safeguards, and other components of activating and using the systems properly.

Please advise what else we can provide and/or how we can improve our training and documentation protocols going forward to ensure that we meet all accreditation standards in this area. I've CC'd Sergeant Ryan Walczak of the Technical Services Unit (the current ALPR Administrator) on this email.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

From: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Sent: Thursday, July 6, 2023 12:04 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: RE: ALPR Operator Training

Good afternoon Sarge,

The standard does not define who an "operator" is. I would assume that it is anyone who is operating a cruiser mounted LPR system. This would be the training during issuance.

The standard below indicates training in the "operator responsibilities" I would view this as issuance including operation and policy responsibilities of the operators.

2.	The agency has a written directive governing the use of License Plate Readers.	**Y N**

3. The written directive addresses:

A	Guidelines for use	**Y N**
B	Operator responsibilities	**Y N**
C	Operator training	**Y N**
D	Data entries	**Y N**
E	Data storage and security	**Y N**
F	Access to data	**Y N**
G	Data retention	**Y N**
4	Agency provided documentation demonstrating LPR Operators received required training. Name(s) sampled:	

Any questions or if I am overlooking something let me know.

Thank you,
BP

Bill Pinkes
Accreditation Manager
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-808-3448

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Wednesday, July 5, 2023 2:32 PM
To: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Subject: Re: ALPR Operator Training

DLt. Pinkes,

Can you please clarify what this standard refers to as an "LPR Operator"? The definition of this term would affect the records provided to satisfy this request.

Thank you,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

From: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Sent: Friday, June 16, 2023 1:42 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: RE: ALPR Operator Training

Hi Sarge,

I have attached a copy of the full Accreditation standard for your reference. Training is required for all LPR operators.

I will need documentation of the training provided for compliance. This can be in the form of the materials presents (powerpoint, lesson plan, manual……) and a sign-in sheet or documentation of how you record the LPR operator has been trained (excel sheet?).

I have also attached a highlighted copy of our current policy that details MSP training requirements on page 7 (highlighted)

Please contact me with any questions you may have. Thank you for reaching out and I appreciate your assistance providing compliance for this issue.

V/R,

Bill P.

Bill Pinkes
Accreditation Manager
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-808-3448

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Wednesday, June 14, 2023 11:18 AM
To: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Subject: Re: ALPR Operator Training

Good morning sir,

Could you please provide further information on any specific accreditation recommendations or requirements as it relates to ALPR cruiser operators, including what type of training is required, who it is required for, what type of documentation is required, or any other considerations we should review?

Respectfully,

Noah

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

From: Bernstein, Eric (POL) <eric.bernstein@pol.state.ma.us>
Sent: Tuesday, June 13, 2023 11:20 PM
To: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Cc: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: RE: ALPR Operator Training

Bill,

Sgt Noah Pak from DHSP coordinates the installation and use of the ALPRs. Traffic Programs just pays for the purchase and maintenance of the units.

He should be able to tell you who currently has working units, and what training they completed.

Respectfully,

Lt. Eric S. Bernstein #2308
Commander, Traffic Programs Section
Commander, Public Order Platoon
Massachusetts State Police
774-462-3762 (office)
[redacted] (cell)
eric.bernstein@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 notify the sender immediately. Thank you.*

From: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Sent: Tuesday, June 13, 2023 1:39 PM
To: Bernstein, Eric (POL) <eric.bernstein@pol.state.ma.us>
Subject: ALPR Operator Training

Good afternoon,

As part of the Accreditation process I am required to provide a proof of compliance that the operators of our ALPR cruiser mounted units have received training.

Could you please provide me with a list of members assigned an ALPR and also a copy of the training/lesson plan provided to the member upon receipt of said equipment.

Should you have any questions, please contact me at your convenience. Thank you in advance for your assistance with this request.

V/R,
Bill P.

Bill Pinkes
Accreditation Manager
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-808-3448


MASSACHUSETTS
STATE
POLICE

From: Pack, Noah (POL)
To: Pinkes, William (POL)
Cc: Walczak, Ryan (POL)
Subject: Re: ALPR Operator Training
Date: Monday, August 7, 2023 3:47:15 PM
Attachments: image001.png
ALPR Active Cruiser & User Training Dates 8-7-23.xlsx

DLt. Pinkes,

Apologies for the delays; I have had limited time at work over the past few weeks.

The Department currently has very few cruiser ALPRs in service. Attached is a record of those who are currently operating a cruiser with a functional and connected ALPR system and their associated training dates. The majority of the Department's cruiser mounted ALPR systems are not currently in service, and those cruisers/users are not reflected on this list. When and if those systems are brought online and placed into service, we will continue to ensure that the users are trained and our documentation is updated.

In past years, training has been done at times by both the systems' vendor (Neology) and our staff. Our user training currently includes, at a minimum, a familiarization on how to use the system, review of our policy with emphasis on the areas that apply to cruiser LPRS, such as hit confirmation procedures/safeguards, and other components of activating and using the systems properly.

Please advise what else we can provide and/or how we can improve our training and documentation protocols going forward to ensure that we meet all accreditation standards in this area. I've CC'd Sergeant Ryan Walczak of the Technical Services Unit (the current ALPR Administrator) on this email.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

From: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Sent: Thursday, July 6, 2023 12:04 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: RE: ALPR Operator Training

Good afternoon Sarge,

The standard does not define who an "operator" is. I would assume that it is anyone who is operating a cruiser mounted LPR system. This would be the training during issuance.

The standard below indicates training in the "operator responsibilities" I would view this as issuance including operation and policy responsibilities of the operators.

2.	The agency has a written directive governing the use of License Plate Readers.	**Y N**

3. The written directive addresses:

A	Guidelines for use	**Y N**
B	Operator responsibilities	**Y N**
C	Operator training	**Y N**
D	Data entries	**Y N**
E	Data storage and security	**Y N**
F	Access to data	**Y N**
G	Data retention	**Y N**
4	Agency provided documentation demonstrating LPR Operators received required training. Name(s) sampled:	

Any questions or if I am overlooking something let me know.

Thank you,
BP

Bill Pinkes
Accreditation Manager
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-808-3448

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Wednesday, July 5, 2023 2:32 PM
To: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Subject: Re: ALPR Operator Training

DLt. Pinkes,

Can you please clarify what this standard refers to as an "LPR Operator"? The definition of this term would affect the records provided to satisfy this request.

Thank you,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

From: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Sent: Friday, June 16, 2023 1:42 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: RE: ALPR Operator Training

Hi Sarge,

I have attached a copy of the full Accreditation standard for your reference. Training is required for all LPR operators.

I will need documentation of the training provided for compliance. This can be in the form of the materials presents (powerpoint, lesson plan, manual……) and a sign-in sheet or documentation of how you record the LPR operator has been trained (excel sheet?).

I have also attached a highlighted copy of our current policy that details MSP training requirements on page 7 (highlighted)

Please contact me with any questions you may have. Thank you for reaching out and I appreciate your assistance providing compliance for this issue.

V/R,
Bill P.

Bill Pinkes
Accreditation Manager
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-808-3448



From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Wednesday, June 14, 2023 11:18 AM
To: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Subject: Re: ALPR Operator Training

Good morning sir,

Could you please provide further information on any specific accreditation recommendations or requirements as it relates to ALPR cruiser operators, including what type of training is required, who it is required for, what type of documentation is required, or any other considerations we should review?

Respectfully,

Noah

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

From: Bernstein, Eric (POL) <eric.bernstein@pol.state.ma.us>
Sent: Tuesday, June 13, 2023 11:20 PM
To: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Cc: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: RE: ALPR Operator Training

Bill,

Sgt Noah Pak from DHSP coordinates the installation and use of the ALPRs. Traffic Programs just pays for the purchase and maintenance of the units.

He should be able to tell you who currently has working units, and what training they completed.

Respectfully,
Lt. Eric S. Bernstein #2308

Commander, Traffic Programs Section
Commander, Public Order Platoon
Massachusetts State Police
774-462-3762 (office)
[redacted] (cell)
eric.bernstein@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 notify the sender immediately. Thank you.*

From: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Sent: Tuesday, June 13, 2023 1:39 PM
To: Bernstein, Eric (POL) <eric.bernstein@pol.state.ma.us>
Subject: ALPR Operator Training

Good afternoon,

As part of the Accreditation process I am required to provide a proof of compliance that the operators of our ALPR cruiser mounted units have received training.

Could you please provide me with a list of members assigned an ALPR and also a copy of the training/lesson plan provided to the member upon receipt of said equipment.

Should you have any questions, please contact me at your convenience. Thank you in advance for your assistance with this request.

V/R,
Bill P.

Bill Pinkes
Accreditation Manager
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-808-3448

From: Pinkes, William (POL)
To: Pack, Noah (POL)
Subject: RE: ALPR Operator Training
Date: Friday, June 16, 2023 1:42:12 PM
Attachments: image001.png
LPR Accreditation Standard.docx
TRF-11 Automatic License Plate Recognition.pdf

Hi Sarge,

I have attached a copy of the full Accreditation standard for your reference. Training is required for all LPR operators.

I will need documentation of the training provided for compliance. This can be in the form of the materials presents (powerpoint, lesson plan, manual……) and a sign-in sheet or documentation of how you record the LPR operator has been trained (excel sheet?).

I have also attached a highlighted copy of our current policy that details MSP training requirements on page 7 (highlighted)

Please contact me with any questions you may have. Thank you for reaching out and I appreciate your assistance providing compliance for this issue.

V/R,
Bill P.

Bill Pinkes
Accreditation Manager
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-808-3448

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Wednesday, June 14, 2023 11:18 AM
To: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Subject: Re: ALPR Operator Training

Good morning sir,

Could you please provide further information on any specific accreditation recommendations or requirements as it relates to ALPR cruiser operators, including what type of training is required, who it is required for, what type of documentation is required, or any other considerations we should review?

Respectfully,

Noah

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

From: Bernstein, Eric (POL) <eric.bernstein@pol.state.ma.us>
Sent: Tuesday, June 13, 2023 11:20 PM
To: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Cc: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: RE: ALPR Operator Training

Bill,

Sgt Noah Pak from DHSP coordinates the installation and use of the ALPRs. Traffic Programs just pays for the purchase and maintenance of the units.

He should be able to tell you who currently has working units, and what training they completed.

Respectfully,
Lt. Eric S. Bernstein #2308
Commander, Traffic Programs Section
Commander, Public Order Platoon
Massachusetts State Police
774-462-3762 (office)
[redacted] (cell)
eric.bernstein@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 notify the sender immediately. Thank you.*

From: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Sent: Tuesday, June 13, 2023 1:39 PM
To: Bernstein, Eric (POL) <eric.bernstein@pol.state.ma.us>
Subject: ALPR Operator Training

Good afternoon,

As part of the Accreditation process I am required to provide a proof of compliance that the operators of our ALPR cruiser mounted units have received training.

Could you please provide me with a list of members assigned an ALPR and also a copy of the training/lesson plan provided to the member upon receipt of said equipment.

Should you have any questions, please contact me at your convenience. Thank you in advance for your assistance with this request.

V/R,
Bill P.

Bill Pinkes
Accreditation Manager
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-808-3448

To: Pack, Noah (POL)
Subject: RE: ALPR Operator Training
Date: Friday, June 16, 2023 1:41:16 PM
Attachments: image001.png
LPR Accreditation Standard.docx

Hi Sarge,

I have attached a copy of the full Accreditation standard for your reference. Training is required for all LPR operators.

I will need documentation of the training provided for compliance. This can be in the form of the materials presents (powerpoint, lesson plan, manual……) and a sign-in sheet or documentation of how you record the LPR operator has been trained (excel sheet?).

I have also attached a highlighted copy of our current policy that details MSP training requirements.

Please contact me with any questions you may have. Thank you for reaching out and I appreciate your assistance providing compliance for this issue.

V/R,
Bill P.

Bill Pinkes
Accreditation Manager
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-808-3448

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Wednesday, June 14, 2023 11:18 AM
To: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Subject: Re: ALPR Operator Training

Good morning sir,

Could you please provide further information on any specific accreditation recommendations or requirements as it relates to ALPR cruiser operators, including what type of training is required, who it is required for, what type of documentation is required, or any other considerations we should review?

Respectfully,

Noah

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

From: Bernstein, Eric (POL) <eric.bernstein@pol.state.ma.us>
Sent: Tuesday, June 13, 2023 11:20 PM
To: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Cc: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: RE: ALPR Operator Training

Bill,

Sgt Noah Pak from DHSP coordinates the installation and use of the ALPRs. Traffic Programs just pays for the purchase and maintenance of the units.

He should be able to tell you who currently has working units, and what training they completed.

Respectfully,

Lt. Eric S. Bernstein #2308
Commander, Traffic Programs Section
Commander, Public Order Platoon
Massachusetts State Police
774-462-3762 (office)
[redacted] (cell)
eric.bernstein@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 notify the sender immediately. Thank you.*

From: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Sent: Tuesday, June 13, 2023 1:39 PM
To: Bernstein, Eric (POL) <eric.bernstein@pol.state.ma.us>
Subject: ALPR Operator Training

Good afternoon,

As part of the Accreditation process I am required to provide a proof of compliance that the operators of our ALPR cruiser mounted units have received training.

Could you please provide me with a list of members assigned an ALPR and also a copy of the training/lesson plan provided to the member upon receipt of said equipment.

Should you have any questions, please contact me at your convenience. Thank you in advance for your assistance with this request.

V/R,
Bill P.

Bill Pinkes
Accreditation Manager
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-808-3448

From: Pack, Noah (POL)
To: Pinkes, William (POL)
Cc: Walczak, Ryan (POL)
Subject: Re: ALPR Operator Training
Date: Friday, September 1, 2023 2:12:08 PM
Attachments: image001.png

DLt. Pinkes,

Just following up on this request. As the LPR program has been transitioned to new management and responsibility (now run by Sgt. Ryan Walczak of the Technical Services Unit), we are working through a number of transitional tasks, including this request regarding training documentation.

There are some other changes going on with the program that will impact user management and training which make this a bit more complicated than it might initially seem. We are working on it, in consideration of the revised definition of what you are looking for and the dynamic nature of the program, and should have something for you soon.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

From: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Sent: Tuesday, August 8, 2023 2:39 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Walczak, Ryan (POL) <ryan.walczak@pol.state.ma.us>
Subject: RE: ALPR Operator Training

That is my error, my misguided thought was that we were utilizing Cruiser Mounted mainly.

The operator should be correctly defined as any employee who utilizes and/or accesses the data collected from an ALPR.

My apologies for any confusion I caused. Thank you for your assistance in addressing this standard to all operators of any ALPR system.

V/R,
Bill P.

Bill Pinkes
Accreditation Manager

Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-808-3448

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Tuesday, August 8, 2023 1:25 PM
To: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Cc: Walczak, Ryan (POL) <ryan.walczak@pol.state.ma.us>
Subject: Re: ALPR Operator Training

DLt. Pinkes,

That is a different area than the cruiser mounted LPRs, which is the reason I inquired as the definition of an LPR operator in an earlier email. Is there a separate standard we should be considering related to that inquiry?

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

From: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Sent: Tuesday, August 8, 2023 1:11 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Walczak, Ryan (POL) <ryan.walczak@pol.state.ma.us>
Subject: RE: ALPR Operator Training

Good afternoon,

Thank you for assisting me with this information. Recognizing that we are utilizing very limited numbers of cruiser mounted ALPR's, I would pose the same questions to ascertain compliance with stationary ALPR systems.

Could you advise the who/what/when related to training for the stationary systems.

Thank you in advance for your assistance gathering this information. Don't hesitate to reach out directly with any questions/concerns either of you may have. I appreciate your help.

V/R,
Bill P.

Bill Pinkes
Accreditation Manager
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-808-3448

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Monday, August 7, 2023 3:47 PM
To: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Cc: Walczak, Ryan (POL) <ryan.walczak@pol.state.ma.us>
Subject: Re: ALPR Operator Training

DLt. Pinkes,

Apologies for the delays; I have had limited time at work over the past few weeks.

The Department currently has very few cruiser ALPRs in service. Attached is a record of those who are currently operating a cruiser with a functional and connected ALPR system and their associated training dates. The majority of the Department's cruiser mounted ALPR systems are not currently in service, and those cruisers/users are not reflected on this list. When and if those systems are brought online and placed into service, we will continue to ensure that the users are trained and our documentation is updated.

In past years, training has been done at times by both the systems' vendor (Neology) and our staff. Our user training currently includes, at a minimum, a familiarization on how to use the system, review of our policy with emphasis on the areas that apply to cruiser LPRS, such as hit confirmation procedures/safeguards, and other components of activating and using the systems properly.

Please advise what else we can provide and/or how we can improve our training and documentation protocols going forward to ensure that we meet all accreditation standards in this area. I've CC'd Sergeant Ryan Walczak of the Technical Services Unit (the current ALPR

Administrator) on this email.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

From: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Sent: Thursday, July 6, 2023 12:04 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: RE: ALPR Operator Training

Good afternoon Sarge,

The standard does not define who an "operator" is. I would assume that it is anyone who is operating a cruiser mounted LPR system. This would be the training during issuance.

The standard below indicates training in the "operator responsibilities" I would view this as issuance including operation and policy responsibilities of the operators.

2.	The agency has a written directive governing the use of License Plate Readers.	**Y N**

3. The written directive addresses:

A	Guidelines for use	**Y N**
B	Operator responsibilities	**Y N**
C	Operator training	**Y N**
D	Data entries	**Y N**
E	Data storage and security	**Y N**
F	Access to data	**Y N**
G	Data retention	**Y N**
4	Agency provided documentation demonstrating LPR Operators received required training. Name(s) sampled:	

Any questions or if I am overlooking something let me know.

Thank you,
BP

Bill Pinkes
Accreditation Manager
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-808-3448

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Wednesday, July 5, 2023 2:32 PM
To: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Subject: Re: ALPR Operator Training

DLt. Pinkes,

Can you please clarify what this standard refers to as an "LPR Operator"? The definition of this term would affect the records provided to satisfy this request.

Thank you,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

From: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Sent: Friday, June 16, 2023 1:42 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: RE: ALPR Operator Training

Hi Sarge,

I have attached a copy of the full Accreditation standard for your reference. Training is required for all LPR operators.

I will need documentation of the training provided for compliance. This can be in the form of the materials presents (powerpoint, lesson plan, manual……) and a sign-in sheet or documentation of how you record the LPR operator has been trained (excel sheet?).

I have also attached a highlighted copy of our current policy that details MSP training requirements on page 7 (highlighted)

Please contact me with any questions you may have. Thank you for reaching out and I appreciate your assistance providing compliance for this issue.

V/R,
Bill P.

Bill Pinkes
Accreditation Manager
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-808-3448

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Wednesday, June 14, 2023 11:18 AM
To: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Subject: Re: ALPR Operator Training

Good morning sir,

Could you please provide further information on any specific accreditation recommendations or requirements as it relates to ALPR cruiser operators, including what type of training is required, who it is required for, what type of documentation is required, or any other considerations we should review?

Respectfully,

Noah

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

From: Bernstein, Eric (POL) <eric.bernstein@pol.state.ma.us>

Sent: Tuesday, June 13, 2023 11:20 PM
To: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Cc: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: RE: ALPR Operator Training

Bill,

Sgt Noah Pak from DHSP coordinates the installation and use of the ALPRs. Traffic Programs just pays for the purchase and maintenance of the units.

He should be able to tell you who currently has working units, and what training they completed.

Respectfully,
Lt. Eric S. Bernstein #2308
Commander, Traffic Programs Section
Commander, Public Order Platoon
Massachusetts State Police
774-462-3762 (office)
[redacted] (cell)
eric.bernstein@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 notify the sender immediately. Thank you.*

From: Pinkes, William (POL) <william.pinkes@pol.state.ma.us>
Sent: Tuesday, June 13, 2023 1:39 PM
To: Bernstein, Eric (POL) <eric.bernstein@pol.state.ma.us>
Subject: ALPR Operator Training

Good afternoon,

As part of the Accreditation process I am required to provide a proof of compliance that the operators of our ALPR cruiser mounted units have received training.

Could you please provide me with a list of members assigned an ALPR and also a copy of the training/lesson plan provided to the member upon receipt of said equipment.

Should you have any questions, please contact me at your convenience. Thank you in advance for your assistance with this request.

V/R,
Bill P.

Bill Pinkes

Accreditation Manager
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-808-3448

From: Cyr, Mark (POL)
To: Condlin, Christopher (POL)
Cc: Powers, Liam (POL); Pack, Noah (POL)
Subject: Re: ALPR Policy Revision Draft
Date: Thursday, May 25, 2023 3:05:46 PM
Attachments: TRF-11 Automatic License Plate Recognition DRAFT 2023 (1) (1).docx

---

Chris,
Please give me a call when you have a chance in regard to this policy (INV 11).

Thank you,
Mark

Lieutenant Colonel Mark D. Cyr #2728
Massachusetts State Police
Division Commander
Division of Homeland Security and Preparedness
508-988-7301 (office)
[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: Cyr, Mark (POL)
Sent: Friday, May 5, 2023 1:51 PM
To: Condlin, Christopher (POL) <Christopher.S.Condlin@pol.state.ma.us>
Cc: Powers, Liam (POL) <Liam.J.Powers@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: ALPR Policy Revision Draft

Good afternoon Chris,
Please find attached the ALPR policy revision draft. I believe it will need some formatting. If possible, can we include it in this quarter's batch awaiting promulgation? Legal has already reviewed and approved. Please do not hesitate to reach out with any questions/concerns.

Thank you,
Mark

Lieutenant Colonel Mark D. Cyr #2728
Massachusetts State Police
Division Commander
Division of Homeland Security and Preparedness
508-988-7301 (office)

[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: Erika M. Warren
To: Fitzgerald, Carol (POL)
Subject: RE: Conference vendor
Date: Thursday, June 15, 2023 11:37:16 AM
Attachments: image001.png

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

Oh ya, SO FUN!!! I make sure to complain to Justin as much as possible about it so he also has to go through it

Maybe October is the sweet spot for the conference!! That's so awesome!!

And maybe it could be ok, but I just have a funny feeling about it. MACA is not the place for that kind of thing. We could have a panel with ALL vendors so questions could be asked and answered at the same time, but not just the two LPRs pitted against each other.

Erika Warren
Criminal Intelligence Specialist
NESPIN
124 Grove St, Suite 105
Franklin, MA 02038
508-530-0565
ewarren@nespin.riss.net
Intel Unit Email: intelunit@nespin.riss.net

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

RISS – A Proven Resource for Law Enforcement

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

This e-mail and any files transmitted with it are confidential or the property of NESPIN, and disclosures or distribution to anyone other than the intended recipient without prior written permission is prohibited. This e-mail is intended solely for the use of the individual or entity to whom this e-mail is addressed. The information contained in this message may contain information that is protected by law. If you are not one of the named recipient(s), you are hereby notified that any disclosure, copying, or distribution is strictly prohibited. If you have reason to believe that you have received this message in error, please notify the sender by replying to the e-mail, calling the sender and deleting this message.

From: Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us>
Sent: Thursday, June 15, 2023 11:33 AM
To: Erika M. Warren <ewarren@nespin.riss.net>
Subject: RE: Conference vendor

LOK right? Still getting used to it! And changing all your documents is a joy too right???? LOL.

I was not a fan of Glen's idea- glad you spoke up. We definitely need to do a punch card and raffle. We are up to SEVEN vendors!!!!!!!

From: Erika M. Warren <ewarren@nespin.riss.net>
Sent: Thursday, June 15, 2023 11:29 AM
To: Fitzgerald, Carol (POL) <Carol.Fitzgerald@pol.state.ma.us>
Subject: RE: Conference vendor

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

Haha my initials!!! Always makes me laugh.

Erika Warren
Criminal Intelligence Specialist
NESPIN
124 Grove St, Suite 105
Franklin, MA 02038
508-530-0565
ewarren@nespin.riss.net
Intel Unit Email: intelunit@nespin.riss.net

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

RISS – A Proven Resource for Law Enforcement

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

This e-mail and any files transmitted with it are confidential or the property of NESPIN, and disclosures or distribution to anyone other than the intended recipient without prior written permission is prohibited. This e-mail is intended solely for the use of the individual or entity to whom this e-mail is addressed. The information contained in this message may contain information that is protected by law. If you are not one of the named recipient(s), you are hereby notified that any disclosure, copying, or distribution is strictly prohibited. If you have reason to believe that you have received this message in error, please notify the sender by replying to the e-mail, calling the sender and deleting this message.

From: Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us>
Sent: Thursday, June 15, 2023 11:28 AM

To: Erika M. Warren <ewarren@nespin.riss.net>; Mills, Glen <gamills@bpd.org>; MACA EBoard (eboard@macrimeanalysts.org) <eboard@macrimeanalysts.org>; djpiehl11 <djpiehl11@gmail.com>; Rob Stering (robbocop@comcast.net) <robbocop@comcast.net>
Subject: RE: Conference vendor

I agree with EW. Could be hairy.

From: Erika M. Warren <ewarren@nespin.riss.net>
Sent: Thursday, June 15, 2023 11:10 AM
To: Mills, Glen <gamills@bpd.org>; Fitzgerald, Carol (POL) <Carol.Fitzgerald@pol.state.ma.us>; MACA EBoard (eboard@macrimeanalysts.org) <eboard@macrimeanalysts.org>; djpiehl11 <djpiehl11@gmail.com>; Rob Stering (robbocop@comcast.net) <robbocop@comcast.net>
Subject: RE: Conference vendor

CAUTION: This email originated from a sender outside of the 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 don't know if I'm a fan of Flock and Motorola on the same panel. In my opinion, it seems like we're encouraging a debate. They would likely be professional, but I can just see it getting a little hairy!

Erika Warren
Criminal Intelligence Specialist
NESPIN
124 Grove St, Suite 105
Franklin, MA 02038
508-530-0565
ewarren@nespin.riss.net
Intel Unit Email: intelunit@nespin.riss.net

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

RISS – A Proven Resource for Law Enforcement

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

This e-mail and any files transmitted with it are confidential or the property of NESPIN, and disclosures or distribution to anyone other than the intended recipient without prior written permission is prohibited. This e-mail is intended solely for the use of the individual or entity to whom this e-mail is addressed. The information contained in this message may contain information that is protected by law. If you are not one of the named recipient(s), you are hereby notified that any disclosure, copying, or distribution is strictly prohibited. If you have reason to believe that you have received this message in error, please notify the sender by replying to the e-mail, calling the sender and deleting this message.

From: Glen A. Mills <gamills@bpd.org>
Sent: Thursday, June 15, 2023 11:01 AM
To: Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us>; MACA EBoard (eboard@macrimeanalysts.org) <eboard@macrimeanalysts.org>; djpiehl11 <djpiehl11@gmail.com>; Rob Stering (robbocop@comcast.net) <robbocop@comcast.net>
Subject: Re: Conference vendor

This is great news.

I think a general panel would be good. If they are not opposed to it perhaps they would allow someone from Flock on the panel along with someone local (MSP) who has used LPR for a long time.

We can say the presentation is sponsored by them as well.

From: Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us>
Sent: Thursday, June 15, 2023 10:48 AM
To: MACA EBoard (eboard@macrimeanalysts.org) <eboard@macrimeanalysts.org>; djpiehl11 <djpiehl11@gmail.com>; Rob Stering (robbocop@comcast.net) <robbocop@comcast.net>
Subject: FW: Conference vendor

Well then ~ so this is the biggest exhibitor sponsor I think we've ever had in history of 23 conferences……..

I'll respond again including the packet which they can select from. I'm assuming their $5K sponsor includes their $700 registration fee.

I'll email her back stating such- we still have plenty of wiggle time. But I guess it's up for some further discussion ~

From: Lisa Benincasa <lisa.benincasa@motorolasolutions.com>
Sent: Tuesday, June 13, 2023 4:30 PM
To: Fitzgerald, Carol (POL) <Carol.Fitzgerald@pol.state.ma.us>
Subject: Re: Conference vendor

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

We would like to sponsor $5000 to the conference. How do we start that process? ALso wanted to know if we could have a panel or discussion time slot to talk about LPR/ALPR and how it helps solve crimes.

My Very Best,

Lisa

Lisa Benincasa
Regional Sales Manager-New England
Motorola Solutions-WatchGuard
Lisa.Benincasa@motorolasolutions.com **978.376.5873 (M)**

Rise to the moment with resilient, reliable, real-time communications in the moments that matter.

On Wed, Jun 7, 2023 at 9:27 AM Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us> wrote:

> Good morning Lisa ~ I hope you're well! My name is Carol Fitzgerald and I am the conference coordinator for the Massachusetts Association of Crime Analysts https://www.macrimeanalysts.org/
>
> We are hosting our annual training conference in October in Plymouth MA and Chris participated as an exhibitor last year and we are hoping Motorola Solutions would be interested in participating again!
>
> Attached is the packet of information for your team to review.
>
> Please let me know if you have any questions and I thank you for your consideration!
>
> Best,
> Carol
>
> ---
>
> **From:** Chris Drake <christopher.drake@motorolasolutions.com>
> **Sent:** Monday, June 5, 2023 4:59 PM
> **To:** Fitzgerald, Carol (POL) <Carol.Fitzgerald@pol.state.ma.us>; Lisa Benincasa <lisa.benincasa@motorolasolutions.com>
> **Subject:** Re: Conference vendor
>
> CAUTION: This email originated from a sender outside of the 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 Carol,
>
> I am no longer the POC for MA. If you want to reach out to Lisa I have included her in this email.

Thank you,

Chris Drake

Regional Sales Manager - (CT,NH,ME)

Mobile Video Solutions

M: **603.205.1845**

On Mon, Jun 5, 2023 at 4:45 PM Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us> wrote:

> Hello Chris! I hope you are well! I wanted to touch base again with our upcoming New England Crime Analysis & Intel Conference and check in to see if Motorola would be interested in being an exhibitor again. I included the info packet for your team to review!
>
> Please let me know if you have any questions! Have a good afternoon Chris and I look forward to hearing from you.
>
> Kind Regards,
> Carol Fitzgerald
> Conference coordinator
>
> Carol Fitzgerald
> Research Analyst III
> Massachusetts State Police
> Commonwealth Fusion Center
> 124 Acton Street, Maynard MA 01754
> 978-451-3714
> Carol.Fitzgerald@pol.state.ma.us
> CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. It may be distributed to state, tribal, or local government law enforcement officials with a need-to-know. Further distribution without CFC authorization is prohibited. 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 the CFC at 978-451-3701 immediately. Thank you.*

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

> *Policy*.

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

From: Fitzgerald, Carol (POL)
To: Erika M. Warren
Subject: RE: Conference vendor
Date: Thursday, June 15, 2023 11:33:00 AM
Attachments: image001.png

LOK right? Still getting used to it! And changing all your documents is a joy too right???? LOL.

I was not a fan of Glen's idea- glad you spoke up. We definitely need to do a punch card and raffle. We are up to SEVEN vendors!!!!!!!

From: Erika M. Warren <ewarren@nespin.riss.net>
Sent: Thursday, June 15, 2023 11:29 AM
To: Fitzgerald, Carol (POL) <Carol.Fitzgerald@pol.state.ma.us>
Subject: RE: Conference vendor

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

Haha my initials!!! Always makes me laugh.

Erika Warren
Criminal Intelligence Specialist
NESPIN
124 Grove St, Suite 105
Franklin, MA 02038
508-530-0565
ewarren@nespin.riss.net
Intel Unit Email: intelunit@nespin.riss.net

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

RISS – A Proven Resource for Law Enforcement

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

This e-mail and any files transmitted with it are confidential or the property of NESPIN, and disclosures or distribution to anyone other than the intended recipient without prior written permission is prohibited. This e-mail is intended solely for the use of the individual or entity to whom this e-mail is addressed. The information contained in this message may contain information that is protected by law. If you are not one of the named recipient(s), you are hereby notified that any disclosure, copying, or distribution is strictly prohibited. If you have reason to believe that you have received this message in error,

please notify the sender by replying to the e-mail, calling the sender and deleting this message.

From: Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us>
Sent: Thursday, June 15, 2023 11:28 AM
To: Erika M. Warren <ewarren@nespin.riss.net>; Mills, Glen <gamills@bpd.org>; MACA EBoard (eboard@macrimeanalysts.org) <eboard@macrimeanalysts.org>; djpiehl11 <djpiehl11@gmail.com>; Rob Stering (robbocop@comcast.net) <robbocop@comcast.net>
Subject: RE: Conference vendor

I agree with EW. Could be hairy.

From: Erika M. Warren <ewarren@nespin.riss.net>
Sent: Thursday, June 15, 2023 11:10 AM
To: Mills, Glen <gamills@bpd.org>; Fitzgerald, Carol (POL) <Carol.Fitzgerald@pol.state.ma.us>; MACA EBoard (eboard@macrimeanalysts.org) <eboard@macrimeanalysts.org>; djpiehl11 <djpiehl11@gmail.com>; Rob Stering (robbocop@comcast.net) <robbocop@comcast.net>
Subject: RE: Conference vendor

CAUTION: This email originated from a sender outside of the 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 don't know if I'm a fan of Flock and Motorola on the same panel. In my opinion, it seems like we're encouraging a debate. They would likely be professional, but I can just see it getting a little hairy!

Erika Warren
Criminal Intelligence Specialist
NESPIN
124 Grove St, Suite 105
Franklin, MA 02038
508-530-0565
ewarren@nespin.riss.net
Intel Unit Email: intelunit@nespin.riss.net

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

RISS – A Proven Resource for Law Enforcement

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

This e-mail and any files transmitted with it are confidential or the property of NESPIN, and disclosures or distribution to

anyone other than the intended recipient without prior written permission is prohibited. This e-mail is intended solely for the use of the individual or entity to whom this e-mail is addressed. The information contained in this message may contain information that is protected by law. If you are not one of the named recipient(s), you are hereby notified that any disclosure, copying, or distribution is strictly prohibited. If you have reason to believe that you have received this message in error, please notify the sender by replying to the e-mail, calling the sender and deleting this message.

From: Glen A. Mills <gamills@bpd.org>
Sent: Thursday, June 15, 2023 11:01 AM
To: Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us>; MACA EBoard (eboard@macrimeanalysts.org) <eboard@macrimeanalysts.org>; djpiehl11 <djpiehl11@gmail.com>; Rob Stering (robbocop@comcast.net) <robbocop@comcast.net>
Subject: Re: Conference vendor

This is great news.

I think a general panel would be good. If they are not opposed to it perhaps they would allow someone from Flock on the panel along with someone local (MSP) who has used LPR for a long time.

We can say the presentation is sponsored by them as well.

From: Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us>
Sent: Thursday, June 15, 2023 10:48 AM
To: MACA EBoard (eboard@macrimeanalysts.org) <eboard@macrimeanalysts.org>; djpiehl11 <djpiehl11@gmail.com>; Rob Stering (robbocop@comcast.net) <robbocop@comcast.net>
Subject: FW: Conference vendor

Well then ~ so this is the biggest exhibitor sponsor I think we've ever had in history of 23 conferences……..

I'll respond again including the packet which they can select from. I'm assuming their $5K sponsor includes their $700 registration fee.

I'll email her back stating such- we still have plenty of wiggle time. But I guess it's up for some further discussion ~

From: Lisa Benincasa <lisa.benincasa@motorolasolutions.com>
Sent: Tuesday, June 13, 2023 4:30 PM
To: Fitzgerald, Carol (POL) <Carol.Fitzgerald@pol.state.ma.us>
Subject: Re: Conference vendor

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

We would like to sponsor $5000 to the conference. How do we start that process? ALso wanted to know if we could have a panel or discussion time slot to talk about LPR/ALPR and how it helps solve

crimes.

My Very Best,

Lisa

Lisa Benincasa
Regional Sales Manager-New England
Motorola Solutions-WatchGuard
Lisa.Benincasa@motorolasolutions.com **978.376.5873 (M)**

Rise to the moment with resilient, reliable, real-time communications in the moments that matter.

On Wed, Jun 7, 2023 at 9:27 AM Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us> wrote:

> Good morning Lisa ~ I hope you're well! My name is Carol Fitzgerald and I am the conference coordinator for the Massachusetts Association of Crime Analysts https://www.macrimeanalysts.org/
>
> We are hosting our annual training conference in October in Plymouth MA and Chris participated as an exhibitor last year and we are hoping Motorola Solutions would be interested in participating again!
>
> Attached is the packet of information for your team to review.
>
> Please let me know if you have any questions and I thank you for your consideration!
>
> Best,
> Carol
>
> ---
>
> **From:** Chris Drake <christopher.drake@motorolasolutions.com>
> **Sent:** Monday, June 5, 2023 4:59 PM
> **To:** Fitzgerald, Carol (POL) <Carol.Fitzgerald@pol.state.ma.us>; Lisa Benincasa <lisa.benincasa@motorolasolutions.com>
> **Subject:** Re: Conference vendor
>
> CAUTION: This email originated from a sender outside of the 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 Carol,

I am no longer the POC for MA. If you want to reach out to Lisa I have included her in this email.

Thank you,

Chris Drake

Regional Sales Manager - (CT,NH,ME)

Mobile Video Solutions

M: **603.205.1845**

On Mon, Jun 5, 2023 at 4:45 PM Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us> wrote:

> Hello Chris! I hope you are well! I wanted to touch base again with our upcoming New England Crime Analysis & Intel Conference and check in to see if Motorola would be interested in being an exhibitor again. I included the info packet for your team to review!
>
> Please let me know if you have any questions! Have a good afternoon Chris and I look forward to hearing from you.
>
> Kind Regards,
> Carol Fitzgerald
> Conference coordinator
>
> Carol Fitzgerald
> Research Analyst III
> Massachusetts State Police
> Commonwealth Fusion Center
> 124 Acton Street, Maynard MA 01754
> 978-451-3714
> Carol.Fitzgerald@pol.state.ma.us
> CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. It may be distributed to state, tribal, or local government law enforcement officials with a need-to-know. Further distribution without CFC authorization is prohibited. 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 the CFC at 978-451-3701 immediately. Thank you.*

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

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

From: Erika M. Warren
To: Fitzgerald, Carol (POL)
Subject: RE: Conference vendor
Date: Thursday, June 15, 2023 11:29:47 AM
Attachments: image001.png

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

Haha my initials!!! Always makes me laugh.

Erika Warren
Criminal Intelligence Specialist
NESPIN
124 Grove St, Suite 105
Franklin, MA 02038
508-530-0565
ewarren@nespin.riss.net
Intel Unit Email: intelunit@nespin.riss.net

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

RISS – A Proven Resource for Law Enforcement

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

This e-mail and any files transmitted with it are confidential or the property of NESPIN, and disclosures or distribution to anyone other than the intended recipient without prior written permission is prohibited. This e-mail is intended solely for the use of the individual or entity to whom this e-mail is addressed. The information contained in this message may contain information that is protected by law. If you are not one of the named recipient(s), you are hereby notified that any disclosure, copying, or distribution is strictly prohibited. If you have reason to believe that you have received this message in error, please notify the sender by replying to the e-mail, calling the sender and deleting this message.

From: Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us>
Sent: Thursday, June 15, 2023 11:28 AM
To: Erika M. Warren <ewarren@nespin.riss.net>; Mills, Glen <gamills@bpd.org>; MACA EBoard (eboard@macrimeanalysts.org) <eboard@macrimeanalysts.org>; djpiehl11 <djpiehl11@gmail.com>; Rob Stering (robbocop@comcast.net) <robbocop@comcast.net>
Subject: RE: Conference vendor

I agree with EW. Could be hairy.

From: Erika M. Warren <ewarren@nespin.riss.net>

Sent: Thursday, June 15, 2023 11:10 AM
To: Mills, Glen <gamills@bpd.org>; Fitzgerald, Carol (POL) <Carol.Fitzgerald@pol.state.ma.us>; MACA EBoard (eboard@macrimeanalysts.org) <eboard@macrimeanalysts.org>; djpiehl11 <djpiehl11@gmail.com>; Rob Stering (robbocop@comcast.net) <robbocop@comcast.net>
Subject: RE: Conference vendor

CAUTION: This email originated from a sender outside of the 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 don't know if I'm a fan of Flock and Motorola on the same panel. In my opinion, it seems like we're encouraging a debate. They would likely be professional, but I can just see it getting a little hairy!

Erika Warren
Criminal Intelligence Specialist
NESPIN
124 Grove St, Suite 105
Franklin, MA 02038
508-530-0565
ewarren@nespin.riss.net
Intel Unit Email: intelunit@nespin.riss.net

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

RISS – A Proven Resource for Law Enforcement

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

This e-mail and any files transmitted with it are confidential or the property of NESPIN, and disclosures or distribution to anyone other than the intended recipient without prior written permission is prohibited. This e-mail is intended solely for the use of the individual or entity to whom this e-mail is addressed. The information contained in this message may contain information that is protected by law. If you are not one of the named recipient(s), you are hereby notified that any disclosure, copying, or distribution is strictly prohibited. If you have reason to believe that you have received this message in error, please notify the sender by replying to the e-mail, calling the sender and deleting this message.

From: Glen A. Mills <gamills@bpd.org>
Sent: Thursday, June 15, 2023 11:01 AM
To: Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us>; MACA EBoard (eboard@macrimeanalysts.org) <eboard@macrimeanalysts.org>; djpiehl11 <djpiehl11@gmail.com>; Rob Stering (robbocop@comcast.net) <robbocop@comcast.net>
Subject: Re: Conference vendor

This is great news.

I think a general panel would be good. If they are not opposed to it perhaps they would allow someone from Flock on the panel along with someone local (MSP) who has used LPR for a long time.

We can say the presentation is sponsored by them as well.

From: Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us>
Sent: Thursday, June 15, 2023 10:48 AM
To: MACA EBoard (eboard@macrimeanalysts.org) <eboard@macrimeanalysts.org>; djpiehl11 <djpiehl11@gmail.com>; Rob Stering (robbocop@comcast.net) <robbocop@comcast.net>
Subject: FW: Conference vendor

Well then ~ so this is the biggest exhibitor sponsor I think we've ever had in history of 23 conferences……..

I'll respond again including the packet which they can select from. I'm assuming their $5K sponsor includes their $700 registration fee.

I'll email her back stating such- we still have plenty of wiggle time. But I guess it's up for some further discussion ~

From: Lisa Benincasa <lisa.benincasa@motorolasolutions.com>
Sent: Tuesday, June 13, 2023 4:30 PM
To: Fitzgerald, Carol (POL) <Carol.Fitzgerald@pol.state.ma.us>
Subject: Re: Conference vendor

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

We would like to sponsor $5000 to the conference. How do we start that process? ALso wanted to know if we could have a panel or discussion time slot to talk about LPR/ALPR and how it helps solve crimes.

My Very Best,

Lisa

Lisa Benincasa
Regional Sales Manager-New England
Motorola Solutions-WatchGuard
Lisa.Benincasa@motorolasolutions.com **978.376.5873 (M)**

Rise to the moment with resilient, reliable, real-time communications in the moments that matter.

On Wed, Jun 7, 2023 at 9:27 AM Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us> wrote:

> Good morning Lisa ~ I hope you're well! My name is Carol Fitzgerald and I am the conference coordinator for the Massachusetts Association of Crime Analysts https://www.macrimeanalysts.org/
>
> We are hosting our annual training conference in October in Plymouth MA and Chris participated as an exhibitor last year and we are hoping Motorola Solutions would be interested in participating again!
>
> Attached is the packet of information for your team to review.
>
> Please let me know if you have any questions and I thank you for your consideration!
>
> Best,
> Carol
>
> ---
>
> **From:** Chris Drake <christopher.drake@motorolasolutions.com>
> **Sent:** Monday, June 5, 2023 4:59 PM
> **To:** Fitzgerald, Carol (POL) <Carol.Fitzgerald@pol.state.ma.us>; Lisa Benincasa <lisa.benincasa@motorolasolutions.com>
> **Subject:** Re: Conference vendor
>
> CAUTION: This email originated from a sender outside of the 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 Carol,
>
> I am no longer the POC for MA. If you want to reach out to Lisa I have included her in this email.
>
> Thank you,
>
> **Chris Drake**
>
> **Regional Sales Manager - (CT,NH,ME)**
>
> **Mobile Video Solutions**

M: **603.205.1845**

On Mon, Jun 5, 2023 at 4:45 PM Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us> wrote:

> Hello Chris! I hope you are well! I wanted to touch base again with our upcoming New England Crime Analysis & Intel Conference and check in to see if Motorola would be interested in being an exhibitor again. I included the info packet for your team to review!
>
> Please let me know if you have any questions! Have a good afternoon Chris and I look forward to hearing from you.
>
> Kind Regards,
> Carol Fitzgerald
> Conference coordinator
>
> Carol Fitzgerald
> Research Analyst III
> Massachusetts State Police
> Commonwealth Fusion Center
> 124 Acton Street, Maynard MA 01754
> 978-451-3714
> Carol.Fitzgerald@pol.state.ma.us
> CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. It may be distributed to state, tribal, or local government law enforcement officials with a need-to-know. Further distribution without CFC authorization is prohibited. 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 the CFC at 978-451-3701 immediately. Thank you.*

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

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

From:	Fitzgerald, Carol (POL)
To:	Erika M. Warren; Mills, Glen; MACA EBoard (eboard@macrimeanalysts.org); djpiehl11; Rob Stering (robbocop@comcast.net)
Subject:	RE: Conference vendor
Date:	Thursday, June 15, 2023 11:28:00 AM
Attachments:	image001.png

I agree with EW. Could be hairy.

From: Erika M. Warren <ewarren@nespin.riss.net>
Sent: Thursday, June 15, 2023 11:10 AM
To: Mills, Glen <gamills@bpd.org>; Fitzgerald, Carol (POL) <Carol.Fitzgerald@pol.state.ma.us>; MACA EBoard (eboard@macrimeanalysts.org) <eboard@macrimeanalysts.org>; djpiehl11 <djpiehl11@gmail.com>; Rob Stering (robbocop@comcast.net) <robbocop@comcast.net>
Subject: RE: Conference vendor

CAUTION: This email originated from a sender outside of the 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 don't know if I'm a fan of Flock and Motorola on the same panel. In my opinion, it seems like we're encouraging a debate. They would likely be professional, but I can just see it getting a little hairy!

Erika Warren
Criminal Intelligence Specialist
NESPIN
124 Grove St, Suite 105
Franklin, MA 02038
508-530-0565
ewarren@nespin.riss.net
Intel Unit Email: intelunit@nespin.riss.net

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

RISS – A Proven Resource for Law Enforcement

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

This e-mail and any files transmitted with it are confidential or the property of NESPIN, and disclosures or distribution to anyone other than the intended recipient without prior written permission is prohibited. This e-mail is intended solely for the use of the individual or entity to whom this e-mail is addressed. The information contained in this message may contain information that is protected by law. If you are not one of the named recipient(s), you are hereby notified that any disclosure, copying, or distribution is strictly prohibited. If you have reason to believe that you have received this message in error,

please notify the sender by replying to the e-mail, calling the sender and deleting this message.

From: Glen A. Mills <gamills@bpd.org>
Sent: Thursday, June 15, 2023 11:01 AM
To: Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us>; MACA EBoard (eboard@macrimeanalysts.org) <eboard@macrimeanalysts.org>; djpiehl11 <djpiehl11@gmail.com>; Rob Stering (robbocop@comcast.net) <robbocop@comcast.net>
Subject: Re: Conference vendor

This is great news.

I think a general panel would be good. If they are not opposed to it perhaps they would allow someone from Flock on the panel along with someone local (MSP) who has used LPR for a long time.

We can say the presentation is sponsored by them as well.

From: Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us>
Sent: Thursday, June 15, 2023 10:48 AM
To: MACA EBoard (eboard@macrimeanalysts.org) <eboard@macrimeanalysts.org>; djpiehl11 <djpiehl11@gmail.com>; Rob Stering (robbocop@comcast.net) <robbocop@comcast.net>
Subject: FW: Conference vendor

Well then ~ so this is the biggest exhibitor sponsor I think we've ever had in history of 23 conferences……..

I'll respond again including the packet which they can select from. I'm assuming their $5K sponsor includes their $700 registration fee.

I'll email her back stating such- we still have plenty of wiggle time. But I guess it's up for some further discussion ~

From: Lisa Benincasa <lisa.benincasa@motorolasolutions.com>
Sent: Tuesday, June 13, 2023 4:30 PM
To: Fitzgerald, Carol (POL) <Carol.Fitzgerald@pol.state.ma.us>
Subject: Re: Conference vendor

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

We would like to sponsor $5000 to the conference. How do we start that process? ALso wanted to know if we could have a panel or discussion time slot to talk about LPR/ALPR and how it helps solve crimes.

My Very Best,

Lisa

Lisa Benincasa
Regional Sales Manager-New England
Motorola Solutions-WatchGuard
Lisa.Benincasa@motorolasolutions.com **978.376.5873 (M)**

Rise to the moment with resilient, reliable, real-time communications in the moments that matter.

On Wed, Jun 7, 2023 at 9:27 AM Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us> wrote:

> Good morning Lisa ~ I hope you're well! My name is Carol Fitzgerald and I am the conference coordinator for the Massachusetts Association of Crime Analysts https://www.macrimeanalysts.org/
>
> We are hosting our annual training conference in October in Plymouth MA and Chris participated as an exhibitor last year and we are hoping Motorola Solutions would be interested in participating again!
>
> Attached is the packet of information for your team to review.
>
> Please let me know if you have any questions and I thank you for your consideration!
>
> Best,
> Carol
>
> ---
>
> **From:** Chris Drake <christopher.drake@motorolasolutions.com>
> **Sent:** Monday, June 5, 2023 4:59 PM
> **To:** Fitzgerald, Carol (POL) <Carol.Fitzgerald@pol.state.ma.us>; Lisa Benincasa <lisa.benincasa@motorolasolutions.com>
> **Subject:** Re: Conference vendor
>
> CAUTION: This email originated from a sender outside of the 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 Carol,
>
> I am no longer the POC for MA. If you want to reach out to Lisa I have included her in this email.

Thank you,

Chris Drake

Regional Sales Manager - (CT,NH,ME)

Mobile Video Solutions

M: **603.205.1845**

On Mon, Jun 5, 2023 at 4:45 PM Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us> wrote:

> Hello Chris! I hope you are well! I wanted to touch base again with our upcoming New England Crime Analysis & Intel Conference and check in to see if Motorola would be interested in being an exhibitor again. I included the info packet for your team to review!
>
> Please let me know if you have any questions! Have a good afternoon Chris and I look forward to hearing from you.
>
> Kind Regards,
> Carol Fitzgerald
> Conference coordinator
>
> Carol Fitzgerald
> Research Analyst III
> Massachusetts State Police
> Commonwealth Fusion Center
> 124 Acton Street, Maynard MA 01754
> 978-451-3714
> Carol.Fitzgerald@pol.state.ma.us
> CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. It may be distributed to state, tribal, or local government law enforcement officials with a need-to-know. Further distribution without CFC authorization is prohibited. 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 the CFC at 978-451-3701 immediately. Thank you.*

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

> *Policy*.

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

From: Erika M. Warren
To: Mills, Glen; Fitzgerald, Carol (POL); MACA EBoard (eboard@macrimeanalysts.org); djpiehl11; Rob Stering (robbocop@comcast.net)
Subject: RE: Conference vendor
Date: Thursday, June 15, 2023 11:11:06 AM
Attachments: image001.png

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

I don't know if I'm a fan of Flock and Motorola on the same panel. In my opinion, it seems like we're encouraging a debate. They would likely be professional, but I can just see it getting a little hairy!

Erika Warren
Criminal Intelligence Specialist
NESPIN
124 Grove St, Suite 105
Franklin, MA 02038
508-530-0565
ewarren@nespin.riss.net
Intel Unit Email: intelunit@nespin.riss.net

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

RISS – A Proven Resource for Law Enforcement

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

This e-mail and any files transmitted with it are confidential or the property of NESPIN, and disclosures or distribution to anyone other than the intended recipient without prior written permission is prohibited. This e-mail is intended solely for the use of the individual or entity to whom this e-mail is addressed. The information contained in this message may contain information that is protected by law. If you are not one of the named recipient(s), you are hereby notified that any disclosure, copying, or distribution is strictly prohibited. If you have reason to believe that you have received this message in error, please notify the sender by replying to the e-mail, calling the sender and deleting this message.

From: Glen A. Mills <gamills@bpd.org>
Sent: Thursday, June 15, 2023 11:01 AM
To: Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us>; MACA EBoard (eboard@macrimeanalysts.org) <eboard@macrimeanalysts.org>; djpiehl11 <djpiehl11@gmail.com>; Rob Stering (robbocop@comcast.net) <robbocop@comcast.net>
Subject: Re: Conference vendor

This is great news.

I think a general panel would be good. If they are not opposed to it perhaps they would allow someone from Flock on the panel along with someone local (MSP) who has used LPR for a long time.

We can say the presentation is sponsored by them as well.

From: Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us>
Sent: Thursday, June 15, 2023 10:48 AM
To: MACA EBoard (eboard@macrimeanalysts.org) <eboard@macrimeanalysts.org>; djpiehl11 <djpiehl11@gmail.com>; Rob Stering (robbocop@comcast.net) <robbocop@comcast.net>
Subject: FW: Conference vendor

Well then ~ so this is the biggest exhibitor sponsor I think we've ever had in history of 23 conferences……..

I'll respond again including the packet which they can select from. I'm assuming their $5K sponsor includes their $700 registration fee.

I'll email her back stating such- we still have plenty of wiggle time. But I guess it's up for some further discussion ~

From: Lisa Benincasa <lisa.benincasa@motorolasolutions.com>
Sent: Tuesday, June 13, 2023 4:30 PM
To: Fitzgerald, Carol (POL) <Carol.Fitzgerald@pol.state.ma.us>
Subject: Re: Conference vendor

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

We would like to sponsor $5000 to the conference. How do we start that process? ALso wanted to know if we could have a panel or discussion time slot to talk about LPR/ALPR and how it helps solve crimes.

My Very Best,

Lisa

Lisa Benincasa
Regional Sales Manager-New England
Motorola Solutions-WatchGuard
Lisa.Benincasa@motorolasolutions.com **978.376.5873 (M)**

Rise to the moment with resilient, reliable, real-time communications in the moments that matter.

On Wed, Jun 7, 2023 at 9:27 AM Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us> wrote:

> Good morning Lisa ~ I hope you're well! My name is Carol Fitzgerald and I am the conference coordinator for the Massachusetts Association of Crime Analysts https://www.macrimeanalysts.org/
>
> We are hosting our annual training conference in October in Plymouth MA and Chris participated as an exhibitor last year and we are hoping Motorola Solutions would be interested in participating again!
>
> Attached is the packet of information for your team to review.
>
> Please let me know if you have any questions and I thank you for your consideration!
>
> Best,
> Carol
>
> ---
>
> **From:** Chris Drake <christopher.drake@motorolasolutions.com>
> **Sent:** Monday, June 5, 2023 4:59 PM
> **To:** Fitzgerald, Carol (POL) <Carol.Fitzgerald@pol.state.ma.us>; Lisa Benincasa <lisa.benincasa@motorolasolutions.com>
> **Subject:** Re: Conference vendor
>
> CAUTION: This email originated from a sender outside of the 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 Carol,
>
> I am no longer the POC for MA. If you want to reach out to Lisa I have included her in this email.
>
> Thank you,
>
> **Chris Drake**
>
> **Regional Sales Manager - (CT,NH,ME)**
>
> **Mobile Video Solutions**

M: **603.205.1845**

On Mon, Jun 5, 2023 at 4:45 PM Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us> wrote:

> Hello Chris! I hope you are well! I wanted to touch base again with our upcoming New England Crime Analysis & Intel Conference and check in to see if Motorola would be interested in being an exhibitor again. I included the info packet for your team to review!
>
> Please let me know if you have any questions! Have a good afternoon Chris and I look forward to hearing from you.
>
> Kind Regards,
> Carol Fitzgerald
> Conference coordinator
>
> Carol Fitzgerald
> Research Analyst III
> Massachusetts State Police
> Commonwealth Fusion Center
> 124 Acton Street, Maynard MA 01754
> 978-451-3714
> Carol.Fitzgerald@pol.state.ma.us
> CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. It may be distributed to state, tribal, or local government law enforcement officials with a need-to-know. Further distribution without CFC authorization is prohibited. 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 the CFC at 978-451-3701 immediately. Thank you.*

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

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

From: Fitzgerald, Carol (POL)
To: Erika M. Warren
Subject: RE: Conference vendor
Date: Thursday, June 15, 2023 11:39:00 AM
Attachments: image001.png

I agree- I don't think MACA is big enough for that and if done incorrectly it could backfire tremendously for us…..I have to review our contract. If we are up to 7 vendors- we are closed to anymore!

From: Erika M. Warren <ewarren@nespin.riss.net>
Sent: Thursday, June 15, 2023 11:37 AM
To: Fitzgerald, Carol (POL) <Carol.Fitzgerald@pol.state.ma.us>
Subject: RE: Conference vendor

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

Oh ya, SO FUN!!! I make sure to complain to Justin as much as possible about it so he also has to go through it

Maybe October is the sweet spot for the conference!! That's so awesome!!

And maybe it could be ok, but I just have a funny feeling about it. MACA is not the place for that kind of thing. We could have a panel with ALL vendors so questions could be asked and answered at the same time, but not just the two LPRs pitted against each other.

Erika Warren
Criminal Intelligence Specialist
NESPIN
124 Grove St, Suite 105
Franklin, MA 02038
508-530-0565
ewarren@nespin.riss.net
Intel Unit Email: intelunit@nespin.riss.net

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

RISS – A Proven Resource for Law Enforcement

Disclaimer: Data in public records, commercially available data sources and the internet can contain errors and are generally not totally free from defect. Data from these sources should not be considered definitively accurate,

and all data we provide to you should be independently verified before taking any action based on the results.

This e-mail and any files transmitted with it are confidential or the property of NESPIN, and disclosures or distribution to anyone other than the intended recipient without prior written permission is prohibited. This e-mail is intended solely for the use of the individual or entity to whom this e-mail is addressed. The information contained in this message may contain information that is protected by law. If you are not one of the named recipient(s), you are hereby notified that any disclosure, copying, or distribution is strictly prohibited. If you have reason to believe that you have received this message in error, please notify the sender by replying to the e-mail, calling the sender and deleting this message.

From: Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us>
Sent: Thursday, June 15, 2023 11:33 AM
To: Erika M. Warren <ewarren@nespin.riss.net>
Subject: RE: Conference vendor

LOK right? Still getting used to it! And changing all your documents is a joy too right???? LOL.

I was not a fan of Glen's idea- glad you spoke up. We definitely need to do a punch card and raffle. We are up to SEVEN vendors!!!!!!!

From: Erika M. Warren <ewarren@nespin.riss.net>
Sent: Thursday, June 15, 2023 11:29 AM
To: Fitzgerald, Carol (POL) <Carol.Fitzgerald@pol.state.ma.us>
Subject: RE: Conference vendor

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

Haha my initials!!! Always makes me laugh.

Erika Warren
Criminal Intelligence Specialist
NESPIN
124 Grove St, Suite 105
Franklin, MA 02038
508-530-0565
ewarren@nespin.riss.net
Intel Unit Email: intelunit@nespin.riss.net

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



RISS – A Proven Resource for Law Enforcement

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

This e-mail and any files transmitted with it are confidential or the property of NESPIN, and disclosures or distribution to anyone other than the intended recipient without prior written permission is prohibited. This e-mail is intended solely for the use of the individual or entity to whom this e-mail is addressed. The information contained in this message may contain information that is protected by law. If you are not one of the named recipient(s), you are hereby notified that any disclosure, copying, or distribution is strictly prohibited. If you have reason to believe that you have received this message in error, please notify the sender by replying to the e-mail, calling the sender and deleting this message.

From: Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us>
Sent: Thursday, June 15, 2023 11:28 AM
To: Erika M. Warren <ewarren@nespin.riss.net>; Mills, Glen <gamills@bpd.org>; MACA EBoard (eboard@macrimeanalysts.org) <eboard@macrimeanalysts.org>; djpiehl11 <djpiehl11@gmail.com>; Rob Stering (robbocop@comcast.net) <robbocop@comcast.net>
Subject: RE: Conference vendor

I agree with EW. Could be hairy.

From: Erika M. Warren <ewarren@nespin.riss.net>
Sent: Thursday, June 15, 2023 11:10 AM
To: Mills, Glen <gamills@bpd.org>; Fitzgerald, Carol (POL) <Carol.Fitzgerald@pol.state.ma.us>; MACA EBoard (eboard@macrimeanalysts.org) <eboard@macrimeanalysts.org>; djpiehl11 <djpiehl11@gmail.com>; Rob Stering (robbocop@comcast.net) <robbocop@comcast.net>
Subject: RE: Conference vendor

CAUTION: This email originated from a sender outside of the 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 don't know if I'm a fan of Flock and Motorola on the same panel. In my opinion, it seems like we're encouraging a debate. They would likely be professional, but I can just see it getting a little hairy!

Erika Warren
Criminal Intelligence Specialist
NESPIN
124 Grove St, Suite 105
Franklin, MA 02038
508-530-0565
ewarren@nespin.riss.net
Intel Unit Email: intelunit@nespin.riss.net

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



RISS – A Proven Resource for Law Enforcement

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

This e-mail and any files transmitted with it are confidential or the property of NESPIN, and disclosures or distribution to anyone other than the intended recipient without prior written permission is prohibited. This e-mail is intended solely for the use of the individual or entity to whom this e-mail is addressed. The information contained in this message may contain information that is protected by law. If you are not one of the named recipient(s), you are hereby notified that any disclosure, copying, or distribution is strictly prohibited. If you have reason to believe that you have received this message in error, please notify the sender by replying to the e-mail, calling the sender and deleting this message.

From: Glen A. Mills <gamills@bpd.org>
Sent: Thursday, June 15, 2023 11:01 AM
To: Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us>; MACA EBoard (eboard@macrimeanalysts.org) <eboard@macrimeanalysts.org>; djpiehl11 <djpiehl11@gmail.com>; Rob Stering (robbocop@comcast.net) <robbocop@comcast.net>
Subject: Re: Conference vendor

This is great news.

I think a general panel would be good. If they are not opposed to it perhaps they would allow someone from Flock on the panel along with someone local (MSP) who has used LPR for a long time.

We can say the presentation is sponsored by them as well.

From: Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us>
Sent: Thursday, June 15, 2023 10:48 AM
To: MACA EBoard (eboard@macrimeanalysts.org) <eboard@macrimeanalysts.org>; djpiehl11 <djpiehl11@gmail.com>; Rob Stering (robbocop@comcast.net) <robbocop@comcast.net>
Subject: FW: Conference vendor

Well then ~ so this is the biggest exhibitor sponsor I think we've ever had in history of 23 conferences……..

I'll respond again including the packet which they can select from. I'm assuming their $5K sponsor includes their $700 registration fee.

I'll email her back stating such- we still have plenty of wiggle time. But I guess it's up for some further discussion ~

From: Lisa Benincasa <lisa.benincasa@motorolasolutions.com>
Sent: Tuesday, June 13, 2023 4:30 PM

To: Fitzgerald, Carol (POL) <Carol.Fitzgerald@pol.state.ma.us>
Subject: Re: Conference vendor

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

We would like to sponsor $5000 to the conference. How do we start that process? ALso wanted to know if we could have a panel or discussion time slot to talk about LPR/ALPR and how it helps solve crimes.

My Very Best,

Lisa

Lisa Benincasa
Regional Sales Manager-New England
Motorola Solutions-WatchGuard
Lisa.Benincasa@motorolasolutions.com **978.376.5873 (M)**

Rise to the moment with resilient, reliable, real-time communications in the moments that matter.

On Wed, Jun 7, 2023 at 9:27 AM Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us> wrote:

> Good morning Lisa ~ I hope you're well! My name is Carol Fitzgerald and I am the conference coordinator for the Massachusetts Association of Crime Analysts https://www.macrimeanalysts.org/
>
> We are hosting our annual training conference in October in Plymouth MA and Chris participated as an exhibitor last year and we are hoping Motorola Solutions would be interested in participating again!
>
> Attached is the packet of information for your team to review.
>
> Please let me know if you have any questions and I thank you for your consideration!
>
> Best,
> Carol
>
> ---
>
> **From:** Chris Drake <christopher.drake@motorolasolutions.com>
> **Sent:** Monday, June 5, 2023 4:59 PM

To: Fitzgerald, Carol (POL) <Carol.Fitzgerald@pol.state.ma.us>; Lisa Benincasa <lisa.benincasa@motorolasolutions.com>
Subject: Re: Conference vendor

CAUTION: This email originated from a sender outside of the 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 Carol,

I am no longer the POC for MA. If you want to reach out to Lisa I have included her in this email.

Thank you,

Chris Drake

Regional Sales Manager - (CT,NH,ME)

Mobile Video Solutions

M: 603.205.1845

On Mon, Jun 5, 2023 at 4:45 PM Fitzgerald, Carol (POL) <carol.fitzgerald@state.ma.us> wrote:

> Hello Chris! I hope you are well! I wanted to touch base again with our upcoming New England Crime Analysis & Intel Conference and check in to see if Motorola would be interested in being an exhibitor again. I included the info packet for your team to review!
>
> Please let me know if you have any questions! Have a good afternoon Chris and I look forward to hearing from you.
>
> Kind Regards,
> Carol Fitzgerald
> Conference coordinator
>
> Carol Fitzgerald
> Research Analyst III
> Massachusetts State Police
> Commonwealth Fusion Center
> 124 Acton Street, Maynard MA 01754
> 978-451-3714

> Carol.Fitzgerald@pol.state.ma.us
> CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. It may be distributed to state, tribal, or local government law enforcement officials with a need-to-know. Further distribution without CFC authorization is prohibited. 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 the CFC at 978-451-3701 immediately. Thank you.*
>
> *For more information on how and why we collect your personal information, please visit our Privacy Policy.*

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

From: Pack, Noah (POL)
To: Cyr, Mark (POL)
Subject: Re: DOT Request
Date: Wednesday, July 5, 2023 2:02:49 PM
Attachments: MSP DHS DOT Collocation Request 7-23 Notes Update2.doc

---

Attached version has a couple corrected typos (if you plan on sending it anywhere) but it is substantively the same. Please let me know if I can provide anything further.

Respectfully,

Noah

From: Pack, Noah (POL)
Sent: Wednesday, July 5, 2023 1:41 PM
To: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Subject: DOT Request

LTC:

Attached is the letter you sent to Foti last October.

Also attached is a summary with history and bullet points that may be helpful in your attempts to move this forward.

Respectfully,

Noah

From: Munyon, Kathryn
To: Pack, Noah (POL)
Subject: RE: LEARN Detection Share Request
Date: Thursday, February 2, 2023 8:17:20 PM
Attachments: image001.png
image002.png
VCSO-Massachusetts State Police ALPR MOU.pdf

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

We would like to start sharing ALPR data with your agency through Vigilant. Please have the attached MOU signed by the appropriate person on your department and returned. Once we have this completed, we will be able to start sharing our information with your agency.

Thank you!

Kathryn Munyon
Senior Intelligence Analyst – Crime Analysis Unit
3701 Las Posas Road
Camarillo, CA 93010
O: (805) 383-8797
C: (805) 767-2012
www.venturasheriff.org
www.applyventurasheriff.org

Law Enforcement Sensitive – For Official Use Only

From: no-reply@learn-nvls.com <no-reply@learn-nvls.com>
Sent: Saturday, December 17, 2022 9:56 AM
To: Munyon, Kathryn <Kathryn.Munyon@ventura.org>
Subject: LEARN Detection Share Request

WARNING: If you believe this message may be malicious use the Phish Alert Button to report it or forward the message to Email.Security@ventura.org.

Dear Kathryn Munyon,

The agency, Massachusetts State Police (MA), has requested that you share your Agency detections from Ventura County Sheriff Department with their agency. To proceed with sharing your detections, please login to your LEARN account and proceed to the Data Sharing utility to accept the share.

Agency: Massachusetts State Police (MA)
Agency Manager: Noah Pack
Email: noah.pack@state.ma.us
Phone: 508-820-2300

Data Sharing Approval

Sincerely,

LEARN Automated Services

From: Commonwealth Fusion Center (POL)
To: Hernandez, Stephen S. (POL)
Subject: Re: LPR Info
Date: Tuesday, November 7, 2023 12:18:26 PM
Attachments: TRF-11 Automatic License Plate Recognition (3).pdf
image.png
image.png

Good Afternoon,

I have attached a copy of the Department's ALPR policy, TRF-11, which outlines the requirements for requesting a historical query and/or hotlist. Below are the relevant sections.

Historical:

Search Procedures

The Commonwealth Watch Center (CWC) and Commonwealth Fusion Center (CFC) shall serve as the primary ALPR resource for the Department. Search requests submitted to the CWC/CFC shall include, at a minimum:

- Case number or reference;
- Type of investigation or reason for request;
- Plate number(s) and vehicle description (if available);
- Requested search time period; and
- Requested search area (devices or region).

Hotlist:

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, missing person, or kidnapping broadcasts or bulletins;
- Incapacitated or endangered persons;
- Be-On-Look-Out (BOLO) broadcasts or other public safety alerts;
- Investigation of terrorist or criminal offenses; or
- Wanted persons, arrest warrants, or search warrants.

Manual entries onto a Hot List shall be:

- Entered with the vehicle description, if available;
- Entered with a case number or reference;
- Updated or removed when information changes, is no longer current, or is no longer necessary or reasonable;
- Given special attention to rental and short-term use vehicles;
- Given special attention to incidents that may be quickly resolved;
- Entered with an automatic expiration date no longer than thirty (30) days; and
- Approved by a supervisor, except in exigent circumstances.

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: Hernandez, Stephen S. (POL) <Stephen.S.Hernandez@pol.state.ma.us>
Sent: Tuesday, November 7, 2023 11:51 AM
To: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Subject: LPR Info

Good afternoon,

What do we need for LPRs now? Report number and Supervisors authorization?

Trooper Stephen S. Hernandez #3815
Massachusetts State Police
Division of Homeland Security & Preparedness
Narcotics Section - Task Force 1
John F. Kennedy Building - Boston

From: Molloy, Joseph
To: Pack, Noah (POL)
Subject: RE: LPR System
Date: Tuesday, May 30, 2023 11:00:01 AM
Attachments: BraintreePD_ALPR_MOU_signed.pdf

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

Hi Noah,

Attached is the signed ALPR_MOU.

I would like to get the following individuals trained:

Joseph Molloy - jmolloy@braintreema.gov
Matthew Crowley – mcrowley@braintreema.gov
Charles Paris – cparis@braintreema.gov
Richard Hale – rhale@braintreema.gov

Thank You.

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Sent: Friday, May 26, 2023 3:39 PM
To: Molloy, Joseph <jmolloy@braintreema.gov>
Subject: LPR System

CAUTION: This email was sent from an external source. Please be extra vigilant when replying, opening attachments or clicking links.

Good afternoon Joe,

We now have the ability for outside agency users to be able to view data from cameras in their jurisdiction. Attached is a copy of the MOU and our current ALPR policy. If this is acceptable to your agency, please sign and return to us. We can then set up a training for a few members of your agency to get access.

All users must receive training, and we do not have the resources to manage a large or a constantly changing pool of users (this applies to our own staff as well). Therefore please select approximately 2-4 users from your agency (we recommend investigations level staff primarily due to their experience).

The training is tentatively scheduled for **June 7 at 10:00 AM**. It will take place remotely via

Teams and will take about 1.5 hours. Users should ideally be at their computers and able to follow along. When available, please send me the names and email addresses of the users selected by your agency.

Respectfully,

Noah

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

From: Salvatore, Justin (POL)
To: Pack, Noah (POL)
Subject: Re: LPR Updates
Date: Sunday, July 9, 2023 8:08:31 PM
Attachments: Salvatore, Justin - Vigilant Vehicle Manager 101.pdf
Salvatore, Justin - Vigilant Vehicle Manager Introduction and User Account Management.pdf

---

Good Evening, Sgt. Pack -

I hope all is going well. Attached are copies of my training certificates for the required Vigilant training courses.

Have a good night.

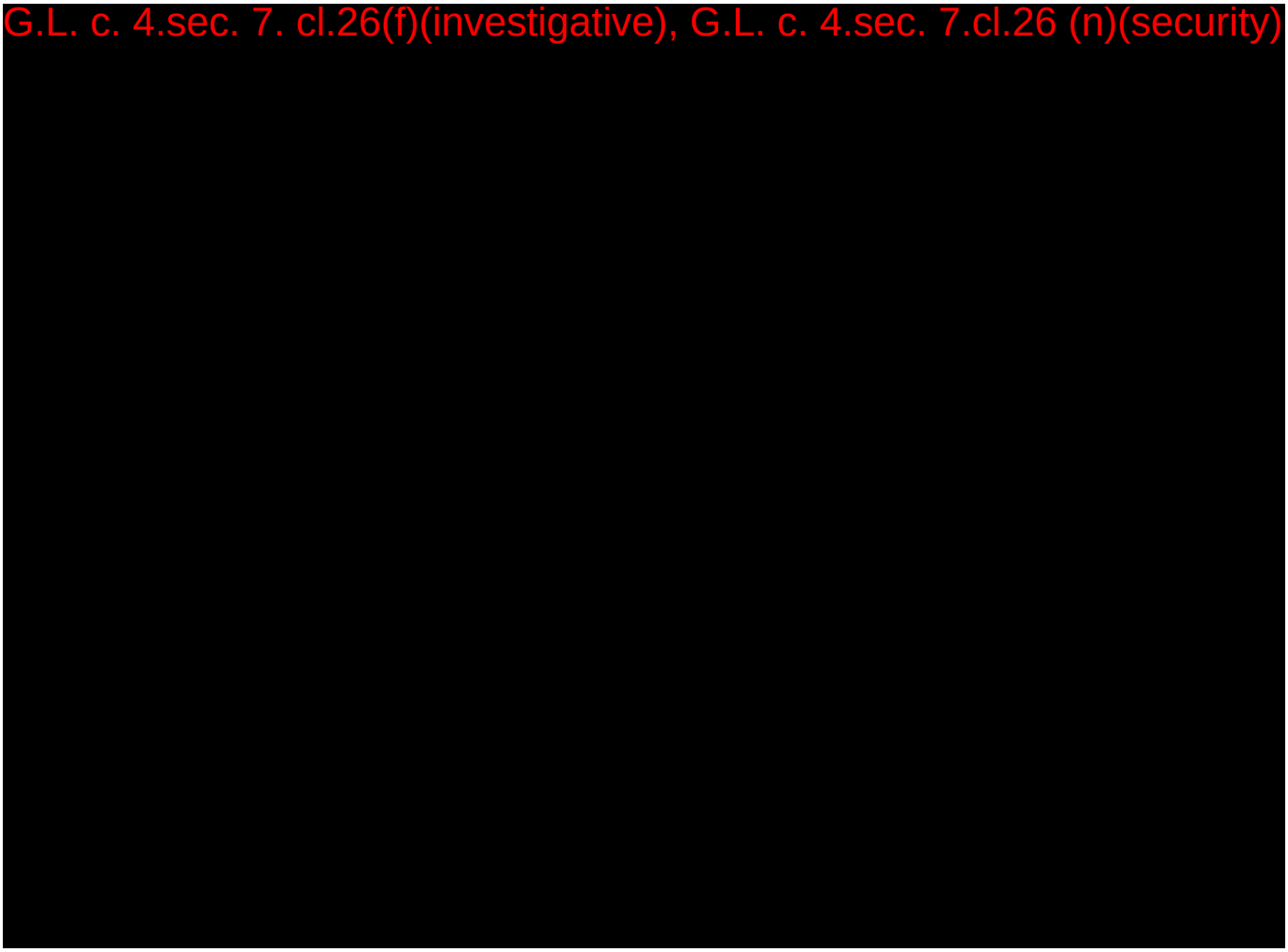
Respectfully,
Justin

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) <noah.pack@pol.state.ma.us>
Sent: Saturday, July 1, 2023 8:25 PM
To: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>; Bennett, Marcy (POL) <Marcy.Bennett@pol.state.ma.us>; Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>; Franquiz, Andrew (POL) <Andrew.Franquiz@pol.state.ma.us>; Grunewald, Brady (POL) <Brady.Grunewald@pol.state.ma.us>; Lee, James (POL) <james.lee@pol.state.ma.us>; Lopez, Adrian (POL) <Adrian.Lopez@pol.state.ma.us>; Mccarron, Richard (POL) <richard.mccarron@pol.state.ma.us>; O'Hara, Edward (POL) <Edward.OHara@pol.state.ma.us>; Palmer, David (POL) <david.palmer@pol.state.ma.us>; Peterson, Kaitlyn H. (POL) <Kaitlyn.H.Peterson@pol.state.ma.us>; Salvatore, Justin (POL) <Justin.Salvatore@pol.state.ma.us>
Cc: Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>; Rudolph, James (POL) <James.Rudolph@pol.state.ma.us>
Subject: LPR Updates

Motorola/Vigilant LEARN

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



Policy Update

The Department's ALPR policy (TRF-11) was officially updated as of June 27, 2023. This policy governs the use of ALPR systems by sworn and civilian members. Please review it (attached) to ensure you are familiar with the most recent version. Many of the updates to this policy directly reflect the best practices that CWC has already doing, such as limiting the scope of searches and the duration of manual hotlist entries. The section titled "Search Procedures" would be particularly relevant to review.

One noteworthy update is that a manual hotlist entry request must be authorized by a supervisor, except in exigent circumstances/emergencies. This can be satisfied in two ways: (1) the request can come directly from a supervisor (Sgt. or above), or (2) the requestor can provide the name of the supervisor who has authorized the request. Until requestors get used to sending this info, you may find yourselves advising them of the requirement and asking for the supervisor's name. For example, something like this might work:

> "We have received your hotlist request. Pursuant to recent MSP policy updates, hotlist requests must be authorized by a supervisor. Please provide the name of the supervisor who has authorized this request."

ALPR Administrator

Thank you for your time and effort as we continue working to improve our Department's LPR system. Some of you know that I have been transferred to a new assignment, and DHS is in the process of selecting someone new to take over the ALPR Administrator role. I will continue to handle these duties through that transition, and as always please feel free to reach out with questions, comments, and success stories.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Investigative Services
Critical Incident Technical Investigations (CITI)

From: Franquiz, Andrew (POL)
To: Pack, Noah (POL)
Subject: Re: LPR Updates
Date: Tuesday, July 4, 2023 10:17:18 PM
Attachments: FRANQUIZ, Andrew - Vigilant Vehicle Manager Introduction User Account Management.pdf
FRANQUIZ, Andrew - Certificate Vigilant Vehicle Manager 101.pdf

---

Good evening,

Please see the attached certificates.

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

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Saturday, July 1, 2023 8:25 PM
To: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>; Bennett, Marcy (POL) <Marcy.Bennett@pol.state.ma.us>; Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>; Franquiz, Andrew (POL) <Andrew.Franquiz@pol.state.ma.us>; Grunewald, Brady (POL) <Brady.Grunewald@pol.state.ma.us>; Lee, James (POL) <james.lee@pol.state.ma.us>; Lopez, Adrian (POL) <Adrian.Lopez@pol.state.ma.us>; Mccarron, Richard (POL) <richard.mccarron@pol.state.ma.us>; O'Hara, Edward (POL) <Edward.OHara@pol.state.ma.us>; Palmer, David (POL) <david.palmer@pol.state.ma.us>; Peterson, Kaitlyn H. (POL) <Kaitlyn.H.Peterson@pol.state.ma.us>; Salvatore, Justin (POL) <Justin.Salvatore@pol.state.ma.us>
Cc: Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>; Rudolph, James (POL) <James.Rudolph@pol.state.ma.us>
Subject: LPR Updates

Motorola/Vigilant LEARN

An LPR camera is now live in the Motorola/Vigilant LPR system, called LEARN, and additional cameras are expected to follow. G.L. c. 4.sec. 7.cl.26 (n)(security) [redacted] For the upcoming events, please be mindful that LPR data may be in one or both of these systems, and hotlist entries should made in both systems to ensure full coverage across the Department's assets.

Most CWC personnel have accounts in LEARN using your .pol email addresses. Please try logging in and setting this account up if you haven't yet done so. If you do not have an account, please go to this link (https://learn-nvls.com/LEARN/gui/index.aspx) and click "Register" to sign up using your G.L. c. 4.sec. 7.cl.26 (n)(sec) Agency manager roles have been assigned to DLt.

Brooks, IA2 Bender, and IA2 Salvatore. They will be asked to assist with managing user accounts for CWC personnel, as they have done for Boss.

Motorola will be sending training staff to GHQ in August or September to provide in-person training. In the mean time, prior to using this system, please access the Motorola/Vigilant Training Academy via the following link: https://vigilant.policeoneacademy.com/ using your LEARN credentials to sign in.

The following short training courses should be completed to provide familiarity with this system and to satisfy our training obligations:

1. Vigilant Vehicle Manager Introduction and User Account Management (approx. 30 minutes)
2. Vigilant Vehicle Manager 101 (approx. 30 minutes)

There are several additional short courses that are optional but that you may find beneficial to your skill with this software. You will receive a certificate by email upon completion of each course. Please forward those to me to keep with training records.

Policy Update

The Department's ALPR policy (TRF-11) was officially updated as of June 27, 2023. This policy governs the use of ALPR systems by sworn and civilian members. Please review it (attached) to ensure you are familiar with the most recent version. Many of the updates to this policy directly reflect the best practices that CWC has already doing, such as limiting the scope of searches and the duration of manual hotlist entries. The section titled "Search Procedures" would be particularly relevant to review.

One noteworthy update is that a manual hotlist entry request must be authorized by a supervisor, except in exigent circumstances/emergencies. This can be satisfied in two ways: (1) the request can come directly from a supervisor (Sgt. or above), or (2) the requestor can provide the name of the supervisor who has authorized the request. Until requestors get used to sending this info, you may find yourselves advising them of the requirement and asking for the supervisor's name. For example, something like this might work:

> "We have received your hotlist request. Pursuant to recent MSP policy updates, hotlist requests must be authorized by a supervisor. Please provide the name of the supervisor who has authorized this request."

ALPR Administrator

Thank you for your time and effort as we continue working to improve our Department's LPR system. Some of you know that I have been transferred to a new assignment, and DHS is in the process of selecting someone new to take over the ALPR Administrator role. I will continue to handle these duties through that transition, and as always please feel free to reach out with questions, comments, and success stories.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Investigative Services
Critical Incident Technical Investigations (CITI)

From: Bender, Sean (POL)
To: Pack, Noah (POL)
Subject: Re: LPR Updates
Date: Sunday, July 2, 2023 11:10:24 AM
Attachments: VSLEA Certificates - Bender, Sean.pdf

Good Morning, Sergeant -

Congratulations on the new assignment. I'm covering the Watch on OT today, so I figured I'd check out those Vigilant Solutions Law Enforcement Academy trainings that you suggested.

Certificates attached.

Have a great rest of your weekend.

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, July 1, 2023 8:25 PM
To: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>; Bennett, Marcy (POL) <Marcy.Bennett@pol.state.ma.us>; Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>; Franquiz, Andrew (POL) <Andrew.Franquiz@pol.state.ma.us>; Grunewald, Brady (POL) <Brady.Grunewald@pol.state.ma.us>; Lee, James (POL) <james.lee@pol.state.ma.us>; Lopez, Adrian (POL) <Adrian.Lopez@pol.state.ma.us>; Mccarron, Richard (POL) <richard.mccarron@pol.state.ma.us>; O'Hara, Edward (POL) <Edward.OHara@pol.state.ma.us>; Palmer, David (POL) <david.palmer@pol.state.ma.us>; Peterson, Kaitlyn H. (POL) <Kaitlyn.H.Peterson@pol.state.ma.us>; Salvatore, Justin (POL) <Justin.Salvatore@pol.state.ma.us>
Cc: Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>; Rudolph, James (POL) <James.Rudolph@pol.state.ma.us>
Subject: LPR Updates

Motorola/Vigilant LEARN

An LPR camera is now live in the Motorola/Vigilant LPR system, called LEARN, and additional cameras are expected to follow. G.L. c. 4.sec. 7.cl.26 (n)(security) [redacted] For the upcoming events, please be mindful that LPR data may be in one or both of these systems, and hotlist entries should made in both systems to ensure full coverage

across the Department's assets.

Most CWC personnel have accounts in LEARN using your .pol email addresses. Please try logging in and setting this account up if you haven't yet done so. If you do not have an account, please go to this link (https://learn-nvls.com/LEARN/gui/index.aspx) and click "Register" to sign up using your .pol email. Agency manager roles have been assigned to DLt. Brooks, IA2 Bender, and IA2 Salvatore. They will be asked to assist with managing user accounts for CWC personnel, as they have done for Boss.

Motorola will be sending training staff to GHQ in August or September to provide in-person training. In the mean time, prior to using this system, please access the Motorola/Vigilant Training Academy via the following link: https://vigilant.policeoneacademy.com/ using your LEARN credentials to sign in.

The following short training courses should be completed to provide familiarity with this system and to satisfy our training obligations:

1. Vigilant Vehicle Manager Introduction and User Account Management (approx. 30 minutes)
2. Vigilant Vehicle Manager 101 (approx. 30 minutes)

There are several additional short courses that are optional but that you may find beneficial to your skill with this software. You will receive a certificate by email upon completion of each course. Please forward those to me to keep with training records.

Policy Update

The Department's ALPR policy (TRF-11) was officially updated as of June 27, 2023. This policy governs the use of ALPR systems by sworn and civilian members. Please review it (attached) to ensure you are familiar with the most recent version. Many of the updates to this policy directly reflect the best practices that CWC has already doing, such as limiting the scope of searches and the duration of manual hotlist entries. The section titled "Search Procedures" would be particularly relevant to review.

One noteworthy update is that a manual hotlist entry request must be authorized by a supervisor, except in exigent circumstances/emergencies. This can be satisfied in two ways: (1) the request can come directly from a supervisor (Sgt. or above), or (2) the requestor can provide the name of the supervisor who has authorized the request. Until requestors get used to sending this info, you may find yourselves advising them of the requirement and asking for the supervisor's name. For example, something like this might work:

"We have received your hotlist request. Pursuant to recent MSP policy updates,

hotlist requests must be authorized by a supervisor. Please provide the name of the supervisor who has authorized this request."

ALPR Administrator

Thank you for your time and effort as we continue working to improve our Department's LPR system. Some of you know that I have been transferred to a new assignment, and DHS is in the process of selecting someone new to take over the ALPR Administrator role. I will continue to handle these duties through that transition, and as always please feel free to reach out with questions, comments, and success stories.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Investigative Services
Critical Incident Technical Investigations (CITI)

From: Brooks, Brian (POL)
To: Pack, Noah (POL)
Subject: RE: LPR Updates
Date: Sunday, July 2, 2023 2:54:00 PM
Attachments: Vigilant.pdf
Vigilant 2.pdf

Ty Noah

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Saturday, July 1, 2023 8:26 PM
To: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>; Bennett, Marcy (POL) <Marcy.Bennett@pol.state.ma.us>; Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>; Franquiz, Andrew (POL) <Andrew.Franquiz@pol.state.ma.us>; Grunewald, Brady (POL) <Brady.Grunewald@pol.state.ma.us>; Lee, James (POL) <james.lee@pol.state.ma.us>; Lopez, Adrian (POL) <Adrian.Lopez@pol.state.ma.us>; Mccarron, Richard (POL) <richard.mccarron@pol.state.ma.us>; O'Hara, Edward (POL) <Edward.OHara@pol.state.ma.us>; Palmer, David (POL) <david.palmer@pol.state.ma.us>; Peterson, Kaitlyn H. (POL) <Kaitlyn.H.Peterson@pol.state.ma.us>; Salvatore, Justin (POL) <Justin.Salvatore@pol.state.ma.us>
Cc: Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>; Rudolph, James (POL) <James.Rudolph@pol.state.ma.us>
Subject: LPR Updates

Motorola/Vigilant LEARN

An LPR camera is now live in the Motorola/Vigilant LPR system, called LEARN, and additional cameras are expected to follow. G.L. c. 4.sec. 7.cl.26 (n)(security) [redacted] For the upcoming events, please be mindful that LPR data may be in one or both of these systems, and hotlist entries should made in both systems to ensure full coverage across the Department's assets.

Most CWC personnel have accounts in LEARN using your .pol email addresses. Please try logging in and setting this account up if you haven't yet done so. If you do not have an account, please go to this link (https://learn-nvls.com/LEARN/gui/index.aspx) and click "Register" to sign up using your .pol email. Agency manager roles have been assigned to DLt. Brooks, IA2 Bender, and IA2 Salvatore. They will be asked to assist with managing user accounts for CWC personnel, as they have done for Boss.

Motorola will be sending training staff to GHQ in August or September to provide in-person training. In the mean time, prior to using this system, please access the Motorola/Vigilant Training Academy via the following link: https://vigilant.policeoneacademy.com/ using your LEARN credentials to sign in.

The following short training courses should be completed to provide familiarity with this system and to satisfy our training obligations:

1. Vigilant Vehicle Manager Introduction and User Account Management (approx. 30 minutes)
2. Vigilant Vehicle Manager 101 (approx. 30 minutes)

There are several additional short courses that are optional but that you may find beneficial to your skill with this software. You will receive a certificate by email upon completion of each course. Please forward those to me to keep with training records.

Policy Update

The Department's ALPR policy (TRF-11) was officially updated as of June 27, 2023. This policy governs the use of ALPR systems by sworn and civilian members. Please review it (attached) to ensure you are familiar with the most recent version. Many of the updates to this policy directly reflect the best practices that CWC has already doing, such as limiting the scope of searches and the duration of manual hotlist entries. The section titled "Search Procedures" would be particularly relevant to review.

One noteworthy update is that a manual hotlist entry request must be authorized by a supervisor, except in exigent circumstances/emergencies. This can be satisfied in two ways: (1) the request can come directly from a supervisor (Sgt. or above), or (2) the requestor can provide the name of the supervisor who has authorized the request. Until requestors get used to sending this info, you may find yourselves advising them of the requirement and asking for the supervisor's name. For example, something like this might work:

> "We have received your hotlist request. Pursuant to recent MSP policy updates, hotlist requests must be authorized by a supervisor. Please provide the name of the supervisor who has authorized this request."

ALPR Administrator

Thank you for your time and effort as we continue working to improve our Department's LPR system. Some of you know that I have been transferred to a new assignment, and DHS is in the process of selecting someone new to take over the ALPR Administrator role. I will continue to handle these duties through that transition, and as always please feel free to reach out with questions, comments, and success stories.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

Division of Investigative Services

Critical Incident Technical Investigations (CITI)

From: Sharon Easley
To: Lorenco, Nicholas (POL); "Richard Easley"; Noe, Vincent (POL)
Cc: Daley, Gretchen (DOT)
Subject: RE: MSP - ALPR Grant Finalizing before closeout 2-1-23
Date: Monday, January 9, 2023 10:58:43 AM
Attachments: FFY2019 Mass Grant Award 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.

Greetings Nick, Happy New Year!

A few thoughts:

- As luck would have it we are working in Quincy all next week (Tues-Friday, 1/17-1/20) so we can meet in person or virtually. I will follow back up with you on some candidate dates/times. If you have a few candidate dates/times that are good for you guys, please let me know and we'll do our best to accommodate your schedule.
- Wanted to ask why you guys are closing out the grant on 2/1/23? The period of performance for this grant goes through the end of Sept 2023 (see attached). Plus there is an option to extend it another year through 9/30/2024. I believe that Mass already did the extension but I'm researching that. It's probably going to be necessary to do another ISA (between RMV & MSP) if the original one has expired.
- How much money is remaining after the camera purchases? How far do you think it can take you guys for keeping camera system up and running? I think the argument can be made that the expenses you are talking about below are part of this project for LPR deployment. We'll need to reach out to FMCSA to get their approval. John Toto is the new FMCSA rep for Mass.
- We are in the process of working with ITD program stakeholders for gathering projects for the 2023 HP-ITD grant application, so it might be that MSP wants to propose a project for O&M for the LPR systems? We can talk about this next week as well. We would need an annual cost estimate when we work on putting together the grant projects proposed for this next funding cycle.

P.S. I didn't respond to Kory since I'm not sure how much he needs to know right now about internal grant/funding discussions. Copying Gretchen for discussion of possible project for next grant cycle.

Dear FMCSA Financial Assistance Award Recipient:

As you may know, the recent Consolidated Appropriations Act, 2021 signed into law by the President on December 27, 2020, provided extensions to the period of performance (POP) to recipients of financial assistance awards (grants and cooperative agreements) that were issued by the Federal Motor Carrier Safety Administration (FMCSA) in ***fiscal years (FY) 2019 and 2020***. The new project period of performance end dates for these awards are as follows:

Grant Program	New FY 2019 POP End Date	New FY 2020 POP End Date
Motor Carrier Safety Assistance Program (MCSAP) ***(Year of Award + Following Two (2) Fiscal Years)***	9/30/2021	9/30/2022
High Priority Grant, Commercial Vehicle Safety (HP-CMV) ***(Year of Award + Following Three (3) Fiscal Years)***	9/30/2022	9/30/2023
High Priority Grant, Innovative Technology Deployment (HP-ITD) ***(Year of Award + Following Five (5) Fiscal Years)***	9/30/2024	9/30/2025
Commercial Driver's License Program Implementation (CDLPI) ***(Year of Award + Following Five (5) Fiscal Years)***	9/30/2024	9/30/2025
Commercial Motor Vehicle Operator Safety Training (CMVOST) ***(Year of Award + Following Two (2) Fiscal Years)***	9/30/2021	9/30/2022

Kind regards,

Sharon

Sharon Easley, Project Manager
E-Squared Engineering
Direct: 703-858-9545 | Mobile: [redacted] | Fax: 703-724-0983
seasley@e-squared.org
www.e-squared.org

From: Lorenco, Nicholas (POL) [mailto:nicholas.lorenco@state.ma.us]
Sent: Monday, January 9, 2023 7:54 AM
To: Sharon Easley <seasley@e-squared.org>; Richard Easley <reasley@e-squared.org>; Noe, Vincent (POL) <vincent.noe@state.ma.us>; Kory Koster <kkoster@329marketinginc.com>
Subject: MSP - ALPR Grant Finalizing before closeout 2-1-23

Good morning Richard and Sharon,

With the closeout of our ITD grant on 2/1/2023 pertaining to the ALPR, I would like to set up a video conference with our installer Kory Koster, Lt Noe, and you for some questions about the remainder of the money and grant fulfillment. During the last few months, we have seen the challenges of this equipment, and Kory has been very accommodating in fulfilling the needs of CVES. In brief, Kory has submitted a proposal of his services which I see necessary to keeping this ALPR program going. Below is Kory's proposal which we are completely unaware of if it would be applicable to the current grant. Please send us some dates for a video conference. Thank you.

"With the purchase of any technology product, consideration needs to be given to the services available to support the product's operation. Available services need to be matched with the product user's operational needs to ensure that investments are maximized through adoption and utilization. When the MA State Police (MSP) purchased the updated Automated License

Plate Recognition (ALPR) systems for its Commercial Vehicle Enforcement Section, efforts were made to ensure that the purchase included annual calibration and software update services to keep in-vehicle components properly aimed and focused and to keep in-vehicle software up to date.

Noticeably absent from MSP's existing service program is any sort of on-demand, component relocation, or user support services that the project's vendor likely did not know were necessary. To address the vendor's oversight, BSA Security, Inc. recommends that MSP consider a battery of additional services that will address the on-demand configuration & programming changes, product relocations/re-installations, and end-user support needs that are now understood to be necessary.

On-demand configuration, programming, and user support services would address the intermediate system change requests that have been experienced and would add on-demand support for active system users to keep systems online, operational, and optimized. Relocation/re-installation services are recommended to address the movement of ALPR components from one location or vehicle to the next due to changing program needs, vehicle accidents, user errors, user support needs, product failures, and or other mishaps."

Trooper Nicholas Lorenco #4165
Massachusetts State Police
Troop-S, Special Operations
Commercial Vehicle Enforcement Section
906 Elm Street
Concord, MA 01742
Section Office: (978) 369-1004
Google Voice: (857)-574-0030
Fax (978) 369-5353
E-Mail: Nicholas.Lorenco@pol.state.ma.us



From:	/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=4424701DE5774B4185F89272D99E162D-MSP2308
To:	Pack, Noah (POL)
Subject:	RE: PBT
Date:	Wednesday, April 26, 2023 4:00:00 PM
Attachments:	Spec Sheet Mobile Camera 2022 01 MPH M7 Elsag ALPR.pdf Presentation Elsag ALPR 2023 01.pdf

Noah,

Great thanks!

Any word about testing the Moto system?

I was at the MA COP show last week and spoke to a rep from ELSAG. They provided the attached info.

If you think it is worth setting up a meeting with them, I have the sales reps info.

Respectfully,

Lt. Eric S. Bernstein #2308
Commander, Traffic Programs Section
Commander, Public Order Platoon
Massachusetts State Police
774-462-3762 (office)
[redacted] (cell)
eric.bernstein@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 notify the sender immediately. Thank you.*

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Wednesday, April 26, 2023 3:45 PM
To: Bernstein, Eric (POL) <eric.bernstein@pol.state.ma.us>
Subject: Re: PBT

Lt, he contacted me directly about it. I will address it.

Respectfully,

Noah

Sergeant Noah H. Pack

Massachusetts State Police
Division of Homeland Security and Preparedness
Office of the Division Commander

From: Bernstein, Eric (POL) <eric.bernstein@pol.state.ma.us>
Sent: Wednesday, April 26, 2023 3:42 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: FW: PBT

Noah,

Looks like this one was in service but now has a new assigned operator. Can you see if it is possible to get it working again? Thanks!

Respectfully,
Lt. Eric S. Bernstein #2308
Commander, Traffic Programs Section
Commander, Public Order Platoon
Massachusetts State Police
774-462-3762 (office)
M.G.L. c. 4,sec. 7,cl.26 (n)(security) (cell)
eric.bernstein@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 notify the sender immediately. Thank you.*

From: Poudrier, Nathaniel (POL) <Nathaniel.P.Poudrier@pol.state.ma.us>
Sent: Tuesday, April 25, 2023 1:17 PM
To: Traffic Programs (POL) <traffic.programs@pol.State.MA.US>
Subject: PBT

Good afternoon,
I was curious to see if I could potentially be issued a PBT for my cruiser. I administer a lot of SFST during the Eve and Mid shifts. I make a lot of traffic stops and I'm often hunting specifically for OUI's during my shift, it would be a very helpful tool for me. Aside of that, I was recently issued a **new cruiser#2080 which is equip with plate readers and need the programing software installed**. Is Traffic Programs where I would get the software from? Please let me know if you are able to help, thank you for your time.

V/r

Trooper Nathaniel Poudrier #4376

Massachusetts State Police

SP Lee (B1)

215 Laurel Street, Route 20,

Lee, MA 02138

(413)243-0600 / SP Lee

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

From: Bernstein, Eric (POL)
To: Pack, Noah (POL)
Subject: RE: PBT
Date: Wednesday, April 26, 2023 4:00:40 PM
Attachments: Spec Sheet Mobile Camera 2022 01 MPH M7 Elsag ALPR.pdf
Presentation Elsag ALPR 2023 01.pdf

Noah,

Great thanks!

Any word about testing the Moto system?

I was at the MA COP show last week and spoke to a rep from ELSAG. They provided the attached info.

If you think it is worth setting up a meeting with them, I have the sales reps info.

Respectfully,

Lt. Eric S. Bernstein #2308
Commander, Traffic Programs Section
Commander, Public Order Platoon
Massachusetts State Police
774-462-3762 (office)
[redacted] (cell)
eric.bernstein@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 notify the sender immediately. Thank you.*

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Wednesday, April 26, 2023 3:45 PM
To: Bernstein, Eric (POL) <eric.bernstein@pol.state.ma.us>
Subject: Re: PBT

Lt, he contacted me directly about it. I will address it.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police

Division of Homeland Security and Preparedness
Office of the Division Commander

From: Bernstein, Eric (POL) <eric.bernstein@pol.state.ma.us>
Sent: Wednesday, April 26, 2023 3:42 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: FW: PBT

Noah,

Looks like this one was in service but now has a new assigned operator. Can you see if it is possible to get it working again? Thanks!

Respectfully,
Lt. Eric S. Bernstein #2308
Commander, Traffic Programs Section
Commander, Public Order Platoon
Massachusetts State Police
774-462-3762 (office)
[redacted] (cell)
eric.bernstein@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 notify the sender immediately. Thank you.*

From: Poudrier, Nathaniel (POL) <Nathaniel.P.Poudrier@pol.state.ma.us>
Sent: Tuesday, April 25, 2023 1:17 PM
To: Traffic Programs (POL) <traffic.programs@pol.State.MA.US>
Subject: PBT

Good afternoon,
I was curious to see if I could potentially be issued a PBT for my cruiser. I administer a lot of SFST during the Eve and Mid shifts. I make a lot of traffic stops and I'm often hunting specifically for OUI's during my shift, it would be a very helpful tool for me. Aside of that, I was recently issued a **new cruiser#2080 which is equip with plate readers and need the programing software installed**. Is Traffic Programs where I would get the software from? Please let me know if you are able to help, thank you for your time.

V/r

Trooper Nathaniel Poudrier #4376

Massachusetts State Police

SP Lee (B1)

215 Laurel Street, Route 20,

Lee, MA 02138

(413)243-0600 / SP Lee

[redacted] / Cell

From: Driscoll, Elaine (EPS)
To: Procopio, David (POL)
Subject: Re: Proposed statement/background + policy
Date: Friday, October 20, 2023 11:24:15 AM
Attachments: image001.png

Ok great. And you would include the policy? I'm headed to a meeting with Gov's now and will seek approval

Sent from my iPhone

> On Oct 20, 2023, at 10:19 AM, Procopio, David (POL) <david.procopio@pol.state.ma.us> wrote:
>
> Here is a proposed statement and two background points, plus the policy. I don't have any answers yet on numbers of times used.
>
> Statement:
> "The ability to query information about vehicles connected to serious crimes, through both the MSP's automated license plate readers and the DOT's tolling gantries, is a valuable tool to assist in capturing dangerous offenders, securing justice for their victims, and protecting public safety and homeland security. The MSP utilizes both systems judiciously and in accordance with state and federal laws and Constitutional rights of individuals."
> -Me
>
> Background:
> -Use of the MSP's ALPR system is governed by a rigorous Departmental policy, TRF-11 (copy attached to this response).
> -MSP investigators do not have direct access to the DOT gantry information, and request such data from the DOT's legal division via a thorough process that ensures all relevant criteria and safeguards are met.
>
> Dave Procopio
> Director, Media Relations Unit
> Massachusetts State Police
> <image001.png>
>
> <TRF-11.pdf>

From: Biagi, Pamela (POL)
To: Silva, Kyra (POL); Comeau, Melissa (POL)
Subject: RE: Purchase Inquiry
Date: Monday, March 6, 2023 7:17:41 PM
Attachments: image001.png
PSE01.pdf
ITC71.pdf

I have used ITC71 for some small ALPR upgrades in the main line appropriation. I have not conducted an RFQ for the upgrades.

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: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Sent: Monday, March 6, 2023 6:18 PM
To: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Cc: Biagi, Pamela (POL) <Pamela.Biagi@pol.state.ma.us>
Subject: RE: Purchase Inquiry

Hi,

We have previously purchased LPR's from BCM, what contract was utilized and what were the contract guidelines in regards to and RFQ?

Thank you

From: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Sent: Monday, March 06, 2023 5:02 PM
To: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Subject: FW: Purchase Inquiry

This is in regards to the Motorola quote from PSE01…

From: Biagi, Pamela (POL) <Pamela.Biagi@pol.state.ma.us>
Sent: Monday, March 6, 2023 4:03 PM
To: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Subject: RE: Purchase Inquiry

We take it on a case-by-case basis.
Sometimes we will reach out to SBPP and SDP vendors.

We never conduct an RFQ on Motorola.

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: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Sent: Monday, March 6, 2023 3:54 PM
To: Biagi, Pamela (POL) <Pamela.Biagi@pol.state.ma.us>
Subject: RE: Purchase Inquiry

Do you think I need to request multiple quotes from vendors or PSE01? The contract user guide is vague.

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: Biagi, Pamela (POL) <Pamela.Biagi@pol.state.ma.us>
Sent: Monday, March 6, 2023 12:01 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Subject: RE: Purchase Inquiry

I m sorry I should have deferred to Melissa for the grant funding as I thought that part was already approved.

From: Biagi, Pamela (POL)
Sent: Monday, March 6, 2023 11:53 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Subject: FW: Purchase Inquiry

Good morning,

This purchase can be made directly off of the PSE01 contract, category 3.

Pam

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Monday, March 6, 2023 11:10 AM
To: Biagi, Pamela (POL) <Pamela.Biagi@pol.state.ma.us>
Cc: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Subject: Purchase Inquiry

Good morning Pam,

We spoke a bit ago about the possibility of making a purchase from Motorola using the PSE01 state contract and approved grant funding (that is nearing the end of its term on June 30). I've been asked to follow-up about this, and I've attached a draft quote for this inquiry. Could you please advise if this purchase can be made directly off the contract or if any requests need to go out first? If I can answer any specific questions about it, please let me know.

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 [redacted]

From: Erez Sharoni
To: Pack, Noah (POL)
Cc: Bob Manfield; Rob Reid
Subject: Re: Rekor LPR
Date: Monday, June 5, 2023 9:53:40 AM
Attachments: image001.png
image002.png
Sample Equipment and Software Master Subscription Agreement 05.02.2022 (2).pdf

---

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

Good morning Sir,

Attached is a sample master subscription agreement (MSA) for our software and hardware. As you are working with Utility Communications, our reseller in MA, they already signed this MSA with us.

I copied Bob Manfield from Utility Communications so check if they will require you to sign any agreement.

Thank you,

Erez Sharoni
Global Sales Director

M 305-394-2294
E esharoni@rekor.ai | W www.rekor.ai

Contact Our Support Center

REKOR
INTELLIGENCE DRIVEN INNOVATION
A NASDAQ COMPANY: REKR

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Date: Tuesday, May 30, 2023 at 17:11
To: Erez Sharoni <esharoni@rekor.ai>
Cc: Bob Manfield <bobm@utilitycommunications.com>, Rob Reid <rreid@rekor.ai>
Subject: Re: Rekor LPR

Thank you, but I'm not referring to purchasing the equipment. I'm referring to accessing and using the software after it is purchased. When we spoke before I believe you referenced a master service agreement or something to that effect. Will that be necessary or did I misunderstand before?

Respectfully,

Sergeant Noah H. Pack

Massachusetts State Police
Division of Homeland Security and Preparedness
Office of the Division Commander

From: Erez Sharoni <esharoni@rekor.ai>
Sent: Tuesday, May 30, 2023 4:18:42 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Bob Manfield <bobm@utilitycommunications.com>; Rob Reid <rreid@rekor.ai>
Subject: Re: Rekor LPR

CAUTION: This email originated from a sender outside of the 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,

As you are going to use utility Communications' MS state contract terms, they already have the MOU signed with us so you will not need to sign anything directly with us.

If you need a copy, I will be more than happy to send you one.

Erez Sharoni
Global Sales Director

M 305-394-2294
E esharoni@rekor.ai | W https://link.edgepilot.com/s/338d1afb/dteIeAa2q0mfbR9D8H_zvA?u=http://www.rekor.ai/

Contact Our Support Center

REKOR
INTELLIGENCE DRIVEN INNOVATION
A NASDAQ COMPANY: REKR

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Date: Tuesday, May 30, 2023 at 13:00
To: Erez Sharoni <esharoni@rekor.ai>
Subject: Re: Rekor LPR

Hello Erez,

Could you please forward me a copy of the agreement or MOU we would be asked to sign if we purchase Rekor equipment or subscriptions? We'd like to review it ahead of time.

Thank you,

Noah

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

From: Erez Sharoni <esharoni@rekor.ai>
Sent: Monday, April 17, 2023 10:29 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Re: Rekor LPR

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

Work for me, sending teams invite for 1.00PM.

Erez Sharoni
Global Sales Director

M 305-394-2294
E esharoni@rekor.ai | W https://link.edgepilot.com/s/43ce1a7c/45tVLQrG5EKKXoGeu5jvSA?u=http://www.rekor.ai/

Contact Our Support Center

REKOR
INTELLIGENCE DRIVEN INNOVATION
A NASDAQ COMPANY: REKR

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Date: Monday, April 17, 2023 at 10:28
To: Erez Sharoni <esharoni@rekor.ai>
Subject: Re: Rekor LPR

Hello Erez,

Thank you the quick response. I have a few brief questions that I'd be interested in discussing with you. How about 1 PM?

Respectfully,

Noah

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

From: Erez Sharoni <esharoni@rekor.ai>
Sent: Monday, April 17, 2023 9:42 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Rekor LPR

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

Good morning Sgt,

John is no longer with Rekor. I will be happy to set up a call with you.

I am available today anytime between 12.00-3.00PM. Please let me know if this works for you and I will send a teams meeting invite.

Thank you,

Erez Sharoni
Global Sales Director

M 305-394-2294
E esharoni@rekor.ai | W https://link.edgepilot.com/s/76e41a3c/Dx3DMUhXuEy2gB0x0ocZJw?u=http://www.rekor.ai/

Contact Our Support Center

REKOR
INTELLIGENCE DRIVEN INNOVATION
A NASDAQ COMPANY: REKR

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Date: Monday, April 17, 2023 at 9:27 AM
To: John Robling <jrobling@rekor.ai>

Subject: Re: Introduction

Good morning John,

Would you be available for a quick call at some point for a Rekor question?

Thank you,

Noah

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

From: John Robling <jrobling@rekor.ai>
Sent: Tuesday, May 31, 2022 8:29 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Egnitz, Brian (POL) <brian.egnitz@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.

Sounds great Noah. I will circle back in a couple weeks if I have not heard from you to kick this off.

Best,
John

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Sent: Friday, May 27, 2022 12:41 PM
To: John Robling <jrobling@rekor.ai>
Cc: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: Introduction

Thank you, John. 30 days should be fine. I'll be unavailable now for about 2 weeks, so I will check in with you then to get it started.

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: Thursday, May 26, 2022 8:11 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 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.

G.L. c. 4. sec. 7.cl. 26 (c)(medical) 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: Lopez, Adrian (POL)
To: Salvatore, Justin (POL)
Subject: Re: Reminder: Boss4
Date: Thursday, February 16, 2023 4:07:18 PM
Attachments: image.png

Thanks for sharing!

From: Salvatore, Justin (POL) <Justin.Salvatore@pol.state.ma.us>
Sent: Thursday, February 16, 2023 3:58 PM
To: Lopez, Adrian (POL) <Adrian.Lopez@pol.state.ma.us>
Subject: Fw: Reminder: Boss4

Adrian,

Below is some guidance Sean sent out regarding the creation of Boss4 LPR hotlists. Just sending as FYI.

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: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Sent: Tuesday, January 24, 2023 6:54 AM
To: POL-DL-SPEAR <POL-DL-SPEAR@MassMail.State.MA.US>
Subject: Reminder: Boss4

Good Morning, All -

Just a reminder, please ensure that when entering hotlists into Boss4, we are all complying with the Department's ALPR policy (TRF-11, attached), as well as the additional recommendations regarding data retention (24-72 hour vs. 30 day hotlist entries). Sgt. Pack **does** perform routine audits of the ALPR system and hotlist entries, and has recently brought to my attention a handful of entries that do not comply with departmental policy.

Minimum Requirements:

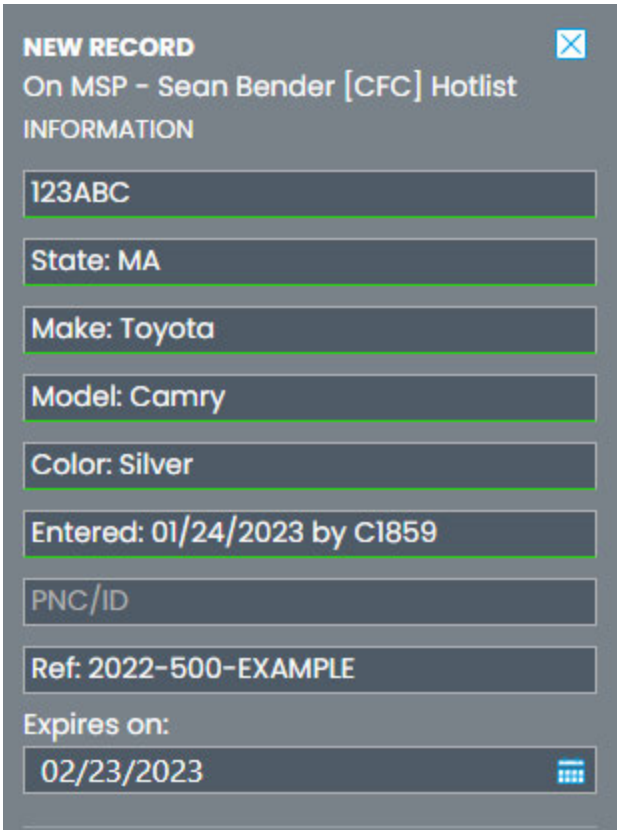
- Authorized purpose (refer to TRF-11)
    - *A case or reference number for a law enforcement investigation or legitimate public safety purpose is REQUIRED.*

- Update/Remove when information changes or is no longer current
    - 30 day expiration date for investigations, 24-72 hours for radio BOLOs, Dispatch requests, Public Safety hotlists etc. After the initial hotlist expires, the investigating officer is responsible for contacting the CFC for a longer term hotlist.
- Entered by:
    - Name or UserID of the user creating the hotlist, for audit purposes.

Additional Recommendations:

- State, Make, Model, Color
    - Including a physical description of the vehicle ensures that if a hit notification is received, recipients can confirm that the vehicle captured matches the suspect vehicle.
- Entered by (Date)
    - This helps us and the recipient to see how recent/relevant a hit notification may be. Agencies often forget to contact the CFC to remove the plate from the hotlist when it is no longer required.

In order to maintain compliance, uniformity, and consistency in our entries, I *highly* recommend utilizing the following format:



Please also ensure that when creating the notification profile that a hotlist is linked to the

notification profile, otherwise, the plate may hit, but the user will not be notified. There are currently a number of notification profiles that are not linked to hotlists, or hotlists that are not linked to notification profiles. These hotlists will not function, even if the plate is captured by an ALPR device.

If you have any questions, please do not hesitate to reach out to myself, Justin, or Sgt. Pack.

Thank you.

Respectfully,

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

From: Pack, Noah (POL)
To: Paul Ulianelli
Subject: Re: Taunton Police ALPR MOUA
Date: Tuesday, March 28, 2023 12:37:23 PM
Attachments: ALPR TENANT MOU 2023.docx

Hi Paul,

Upon review of the ALPR MOU, we need to update the new Colonel's name before I can submit it for his signature. I've attached the new version. Would you kindly be able to have this one signed? I will then submit it for signature on our end and get it back to you as soon as I can.

Respectfully,

Noah

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

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Tuesday, March 21, 2023 3:39 PM
To: Paul Ulianelli <pulianelli@tauntonpd.com>
Subject: Re: Taunton Police ALPR MOUA

Hi Paul,

I will prepare a request to forward this for the colonel's signature. It will probably take a few weeks to get it up and back.

When you are ready to try to link the cruisers, we can set up a call to give it a shot. My next availability will be the first week in April as I'm tied up in court for much of this and next week. I will only be able to help set the configuration settings, and any hardware or software issues will have to go through Kory.

Respectfully,

Noah

Sergeant Noah H. Pack

Massachusetts State Police
Division of Homeland Security and Preparedness
Office of the Division Commander

From: Paul Ulianelli <pulianelli@tauntonpd.com>
Sent: Tuesday, March 21, 2023 11:47 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Taunton Police ALPR MOUA

CAUTION: This email originated from a sender outside of the 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 Sgt Pack,

We've been notified that we will be CJIS audited and one of the documents they will want to see is the ALPR MOUA.

I have a signed copy by my Chief, however, I do not have Colonel Mason's signature.

Who do I submit this MOUA to to have the Colonel's signature?

I attached the MOUA that is signed by my Chief.

Also, we currently have both cruisers sitting in our lot so we can attempt to get the ALPR system operative at some point.

Thank you,

PAUL

PAUL A. ULIANELLI
Computer Systems Administrator
Taunton Police Department
23 Summer St Taunton, MA 02780
Office: (774) 406-4396
Mobile: [redacted] G.L. c. 4,sec. 7,cl.26 (n)(security)

From: Paul Ulianelli
To: Pack, Noah (POL)
Subject: Re: Taunton Police ALPR MOUA
Date: Tuesday, March 28, 2023 1:29:24 PM
Attachments: StatePolice ALPR MOUA_03282023.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 Noah,

Here is the new MOUA signed by my Chief today. Can you forward Col Mawn for his signature and send it back to me?

Thank you,

PAUL

PAUL A. ULIANELLI
Computer Systems Administrator
Taunton Police Department
23 Summer St Taunton, MA 02780
Office: (774) 406-4396
Mobile: [redacted] G.L. c. 4,sec. 7,cl.26 (n)(security)

On Tue, Mar 28, 2023 at 12:37 PM Pack, Noah (POL) <noah.pack@state.ma.us> wrote:

> Hi Paul,
>
> Upon review of the ALPR MOU, we need to update the new Colonel's name before I can submit it for his signature. I've attached the new version. Would you kindly be able to have this one signed? I will then submit it for signature on our end and get it back to you as soon as I can.
>
> Respectfully,
>
> Noah
>
> **Sergeant Noah H. Pack**
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> Office of the Division Commander
>
> ---
>
> **From:** Pack, Noah (POL) <noah.pack@pol.state.ma.us>
> **Sent:** Tuesday, March 21, 2023 3:39 PM

To: Paul Ulianelli <pulianelli@tauntonpd.com>
Subject: Re: Taunton Police ALPR MOUA

Hi Paul,

I will prepare a request to forward this for the colonel's signature. It will probably take a few weeks to get it up and back.

When you are ready to try to link the cruisers, we can set up a call to give it a shot. My next availability will be the first week in April as I'm tied up in court for much of this and next week. I will only be able to help set the configuration settings, and any hardware or software issues will have to go through Kory.

Respectfully,

Noah

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

From: Paul Ulianelli <pulianelli@tauntonpd.com>
Sent: Tuesday, March 21, 2023 11:47 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Taunton Police ALPR MOUA

CAUTION: This email originated from a sender outside of the 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 Sgt Pack,

We've been notified that we will be CJIS audited and one of the documents they will want to see is the ALPR MOUA.

I have a signed copy by my Chief, however, I do not have Colonel Mason's signature.

Who do I submit this MOUA to to have the Colonel's signature?

I attached the MOUA that is signed by my Chief.

Also, we currently have both cruisers sitting in our lot so we can attempt to get the ALPR system operative at some point.

Thank you,

PAUL

PAUL A. ULIANELLI
Computer Systems Administrator
Taunton Police Department
23 Summer St Taunton, MA 02780
Office: (774) 406-4396
Mobile: [redacted]

To:	Mcnamara, Sean (POL)
Cc:	Manning, David (POL)
Subject:	RE: TopGun Slidedeck
Date:	Monday, September 11, 2023 11:56:15 AM
Attachments:	TECHNICAL SERVICES UNIT OVERVIEW.pptx

From: Mcnamara, Sean (POL) <sean.mcnamara@pol.state.ma.us>
Sent: Monday, September 11, 2023 11:10 AM
To: George, Michael (POL) <Michael.George@pol.state.ma.us>
Cc: Manning, David (POL) <david.manning@pol.state.ma.us>
Subject: TopGun Slidedeck

Good morning. Please see attached for the slide deck for TopGun.

I'll tighten up the site survey slide, and make adjustments as you see fit. Please review and advise.

Respectfully submitted,

Tpr. Sean P. McNamara
Massachusetts State Police
Division of Homeland Security and Preparedness
Technical Services Unit
978.771.2924 (c)
sean.mcnamara@pol.state.ma.us

From:	George, Michael (POL)
To:	Mcnamara, Sean (POL)
Cc:	Manning, David (POL)
Subject:	RE: TopGun Slidedeck
Date:	Monday, September 11, 2023 11:59:07 AM
Attachments:	TSU TopGun presentation draft.pptx TECHNICAL SERVICES UNIT OVERVIEW.pptx

Made a few changes – looks great, add a few more pics and run with it

Also added the one I did a few months ago to steal from in the future – will put both on TSU Teams account after the presentation

---

From: Mcnamara, Sean (POL) <sean.mcnamara@pol.state.ma.us>
Sent: Monday, September 11, 2023 11:10 AM
To: George, Michael (POL) <Michael.George@pol.state.ma.us>
Cc: Manning, David (POL) <david.manning@pol.state.ma.us>
Subject: TopGun Slidedeck

Good morning. Please see attached for the slide deck for TopGun.

I'll tighten up the site survey slide, and make adjustments as you see fit. Please review and advise.

Respectfully submitted,

Tpr. Sean P. McNamara
Massachusetts State Police
Division of Homeland Security and Preparedness
Technical Services Unit
978.771.2924 (c)
sean.mcnamara@pol.state.ma.us

From: Gouveia, Kim (NOR)
To: Burton, Ray (POL)
Subject: RE: Training
Date: Tuesday, February 7, 2023 9:49:17 AM
Attachments: 2022-2023 Police Training Manual.pdf
SW Training Agenda 2.8.23 - PDF.pdf
image001.png

Hello,

I added you to our list for future trainings. Attached is the 2022-2023 police training manual. Would you like to attend tomorrows training by ZOOM? I can send you the link if you like. I attached the agenda so you can take a look. Thank you!

Kim

From: Burton, Ray (POL) <ray.burton@pol.state.ma.us>
Sent: Monday, February 06, 2023 6:38 PM
To: Johnsen, Melissa (NOR) <melissa.johnsen@mass.gov>
Cc: Gouveia, Kim (NOR) <kim.gouveia@mass.gov>
Subject: Re: Training

Thank you very much.

Sorry for the delayed responses.

Stay safe,

Ray

Trooper Ray Burton #3544
Massachusetts State Police
Division of Homeland Security
Narcotics Section/ DOC Intelligence Unit
50 Maple Street, Milford, MA 01757
[redacted] Cell
(508) 473-9509 Office
(508) 422-3652 Fax

From: Johnsen, Melissa (NOR) <melissa.johnsen@mass.gov>
Sent: Thursday, January 12, 2023 9:20 AM
To: Burton, Ray (POL) <ray.burton@pol.state.ma.us>
Cc: Gouveia, Kim (NOR) <kim.gouveia@mass.gov>

Subject: RE: Training

Hello Ray, yes, we will put you on the list. In fact, we have a search warrant training coming up on February 8th. I've cc'd Kim Gouveia so that she can send you the registration information.

Attached please find the 2022-2023 Police Training Manual. Feel free to contact me if you have any questions.

Melissa

From: Burton, Ray (POL) <ray.burton@pol.state.ma.us>
Sent: Wednesday, January 11, 2023 8:34 PM
To: Johnsen, Melissa (NOR) <melissa.johnsen@mass.gov>
Subject: Training

Good evening,

I am emailing to see how I get on the email list for trainings from your office and also to get a copy of the criminal law and procedure book?

On the off chance I am emailing the wrong person can you please let me know who I should email if you who I should contact?

Thank you,

Ray

Trooper Ray Burton #3544
Massachusetts State Police
Division of Homeland Security
Narcotics Section/ DOC Intelligence Unit
50 Maple Street, Milford, MA 01757
[redacted] Cell
(508) 473-9509 Office
(508) 422-3652 Fax

From: Pack, Noah (POL)
To: JAMES DOWLING
Subject: Re: Updates
Date: Thursday, June 15, 2023 4:03:56 PM
Attachments: Offer Addenda – LinC Non-MSI Camera LPR Hosting ES.pdf

---

Please see attached.

Respectfully,

Noah

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

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, June 15, 2023 3:40 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Re: Updates

CAUTION: This email originated from a sender outside of the 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, we are in agreement. If you could send over the signed one page doc today, that would be helpful. Thanks.

Jim

On Thu, Jun 15, 2023 at 9:31 AM Pack, Noah (POL) <noah.pack@state.ma.us> wrote:

> Hi Jim,
>
> It's our understanding that our purchase for the LPR cameras and enclosures to be provided by GTBM includes all associated costs for the purchased equipment (except for cellular service, which we will provide), and it will be fully operational and connected through the end of our existing contract period with Motorola for access to the LEARN database ending in March 2027.
>
> In regards to the LinC form, it appears to be a general statement of Motorola's fees for licensing outside cameras and purchasing cellular service, if desired. Based on this approved purchase, we do not expect and are not authorizing or agreeing to any additional fees/costs for the items in this purchase, including the continuation or institution of any recurring

fees after the end of the contract period or outside of the purchased equipment/services, as we would have to seek funding and approval for any such purchases.

If the above is correct and agreed by Motorola, we can return this form for your files.

Respectfully,

Noah

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

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Friday, June 2, 2023 11:55 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: sam.rabadi@motorolasolutions.com <sam.rabadi@motorolasolutions.com>; Lisa Benincasa <lisa.benincasa@motorolasolutions.com>
Subject: Re: Updates

CAUTION: This email originated from a sender outside of the 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, sorry this is taking a little longer than normal as several key people are traveling this week. I'll try to have completed asap.

On a different note, could you please sign the attached doc which our admin needs for the the licensing of the cameras GTBM is providing as part of the covert enclosures. Thanks.

Jim

On Fri, Jun 2, 2023 at 11:37 AM Pack, Noah (POL) <noah.pack@state.ma.us> wrote:

> Hi all,
>
> Following up on these quotes. Thank you again for all your help.
>
> Respectfully,
>
> Noah
>
> **Sergeant Noah H. Pack**
> Massachusetts State Police

Division of Homeland Security and Preparedness
Office of the Division Commander

From: Pack, Noah (POL)
Sent: Wednesday, May 24, 2023 4:51 PM
To: JAMES DOWLING <jdowling@motorolasolutions.com>; sam.rabadi@motorolasolutions.com <sam.rabadi@motorolasolutions.com>; Lisa Benincasa <lisa.benincasa@motorolasolutions.com>
Subject: Updates

Hi all:

Checking in regarding quotes for the newest two sites, equipment integration with LEARN, and a date for install of demo mobile system. Thank you all very much.

Respectfully,

Noah

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

--
Jim Dowling
Senior 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 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.

From: Bender, Sean (POL)
To: POL-DL-SPEAR
Subject: Reminder: Boss4
Date: Tuesday, January 24, 2023 6:54:52 AM
Attachments: TRF-11 Automatic License Plate Recognition (1).pdf
image.png

Good Morning, All -

Just a reminder, please ensure that when entering hotlists into Boss4, we are all complying with the Department's ALPR policy (TRF-11, attached), as well as the additional recommendations regarding data retention (24-72 hour vs. 30 day hotlist entries). Sgt. Pack **does** perform routine audits of the ALPR system and hotlist entries, and has recently brought to my attention a handful of entries that do not comply with departmental policy.

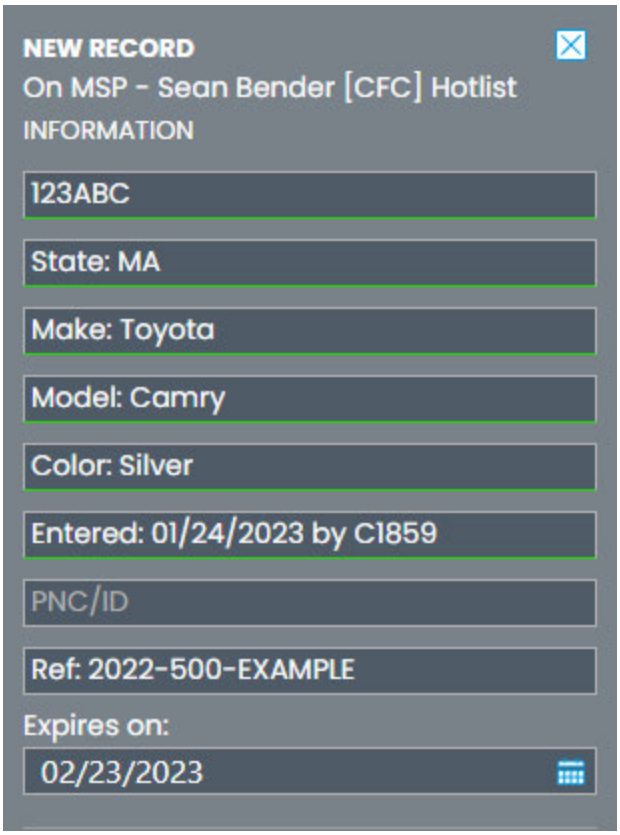
Minimum Requirements:

- Authorized purpose (refer to TRF-11)
  - *A case or reference number for a law enforcement investigation or legitimate public safety purpose is REQUIRED.*
- Update/Remove when information changes or is no longer current
  - 30 day expiration date for investigations, 24-72 hours for radio BOLOs, Dispatch requests, Public Safety hotlists etc. After the initial hotlist expires, the investigating officer is responsible for contacting the CFC for a longer term hotlist.
- Entered by:
  - Name or UserID of the user creating the hotlist, for audit purposes.

Additional Recommendations:

- State, Make, Model, Color
  - Including a physical description of the vehicle ensures that if a hit notification is received, recipients can confirm that the vehicle captured matches the suspect vehicle.
- Entered by (Date)
  - This helps us and the recipient to see how recent/relevant a hit notification may be. Agencies often forget to contact the CFC to remove the plate from the hotlist when it is no longer required.

In order to maintain compliance, uniformity, and consistency in our entries, I *highly* recommend utilizing the following format:



Please also ensure that when creating the notification profile that a hotlist is linked to the notification profile, otherwise, the plate may hit, but the user will not be notified. There are currently a number of notification profiles that are not linked to hotlists, or hotlists that are not linked to notification profiles. These hotlists will not function, even if the plate is captured by an ALPR device.

If you have any questions, please do not hesitate to reach out to myself, Justin, or Sgt. Pack.

Thank you.

Respectfully,

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

From: Ayers, Kathleen
To: Hynes, Allison E (POL)
Subject: Some flock camera materials
Date: Monday, February 6, 2023 4:24:25 PM
Attachments: A&O 13.16.2 LPRs.pdf
A&O 16.1.3 Selective Traffic Enforcement.pdf
A&O 16.6.1 Speed Monitoring.pdf
Executed LPR MOU Marlborough Nov 2021.pdf
ALPR Final.pdf
2019-118.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.

… in case these aid in our discussion tomorrow. We call them LPRs (license plate readers)!

Thank you,

Kate Ayers
Staff Attorney 2
Department of Emergency Services and Public Protection
Phone: (860)-685-8150
Fax: (860)-685-8611
kathleen.ayers@ct.gov

NOTICE: This e-mail transmission and any accompanying attachments may contain confidential or privileged information. They are intended for use by the individual or entity named on this e-mail transmission. If you are not the intended recipient, you are not authorized to disclose, copy, distribute or use, in any manner, the contents of this information. If you have received this e-mail transmission in error, please notify us by e-mail immediately.

From: Procopio, David (POL)
To: Will Katcher
Cc: Driscoll, Elaine (EPS)
Subject: Statement and Policy
Date: Friday, October 20, 2023 4:54:23 PM
Attachments: TRF-11.pdf

Will, here is a statement (please attribute to me) and some background points. Our comprehensive ALPR policy is also included.

The ability to query information about vehicles connected to serious crimes, through both the MSP's automated license plate readers and the DOT's tolling gantries, is a valuable tool to assist in capturing dangerous offenders, securing justice for their victims, and protecting public safety and homeland security. The MSP utilizes both systems judiciously and in accordance with state and federal laws and Constitutional rights of individuals.
-Dave Procopio

Background:
-Use of the MSP's ALPR system is governed by a rigorous Departmental policy, TRF-11 (copy attached to this response).
-MSP investigators do not have direct access to the DOT gantry information, and request such data from the DOT's legal division via a thorough process that ensures all relevant criteria and safeguards are met.

Dave Procopio
Director, Media Communications
Massachusetts State Police

From: Paul Ulianelli
To: Pack, Noah (POL)
Subject: Taunton Police ALPR MOUA
Date: Tuesday, March 21, 2023 11:51:40 AM
Attachments: MOUA_Signed.pdf

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

Hi Sgt Pack,

We've been notified that we will be CJIS audited and one of the documents they will want to see is the ALPR MOUA.

I have a signed copy by my Chief, however, I do not have Colonel Mason's signature.

Who do I submit this MOUA to to have the Colonel's signature?

I attached the MOUA that is signed by my Chief.

Also, we currently have both cruisers sitting in our lot so we can attempt to get the ALPR system operative at some point.

Thank you,

PAUL

PAUL A. ULIANELLI
Computer Systems Administrator
Taunton Police Department
23 Summer St Taunton, MA 02780
Office: (774) 406-4396
Mobile: [redacted] G.L. c. 4.sec. 7.cl.26 (n)(security)

From: Strategic Planning (POL)
Subject: TRF-11 Automatic License Plate Recognition Policy
Date: Tuesday, June 27, 2023 1:45:34 PM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

Please be advised that the following General Order has been promulgated and posted on PowerDMS. This is a revised version of TRF-11. Please use the comparison feature within PowerDMS to view the changes before signing off on the policy.

TRF-11 Automatic License Plate Recognition Policy

PowerDMS Location:

Documents

Policy and Procedure/Rules & Regulations

Policy and Procedure Documents

TRF-11

Strategic Planning and Analysis Section
Office of the Superintendent
470 Worcester Road
Framingham, Massachusetts 01702

From: Strategic Planning (POL)
To: POL-DL-All Users
Subject: TRF-11 Automatic License Plate Recognition
Date: Tuesday, June 27, 2023 1:56:23 PM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

Please be advised that the following General Order has been promulgated and posted to PowerDMS. This is a revised version of TRF-11. Please use the comparison feature withing PowerDMS to view the changes prior to signing off on the policy.

TRF-11 Automatic License Plate Recognition
PowerDMS location:
Documents
Policy and Procedure / Rules and Regulations
Policy and Procedure Documents
TRF-11

Strategic Planning and Analysis Section
Office of the Superintendent
470 Worcester Road
Framingham, MA 01702

From: Strategic Planning (POL)
To: POL-DL-All Users
Subject: TRF-11 Automatic License Plate Recognition
Date: Tuesday, June 27, 2023 2:04:53 PM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

Please be advised that the following General Order has been promulgated and posted to PowerDMS. This is a revised version of TRF-11. Please use the comparison feature within PowerDMS to view the changes prior to signing off on the policy.

TRF-11 Automatic License Plate Recognition
PowerDMS location:
Documents
Policy and Procedure / Rules and Regulations
Policy and Procedure Documents
TRF-11

Strategic Planning and Analysis Section
Office of the Superintendent
470 Worcester Road
Framingham, MA 01702

From: Condlin, Christopher (POL)
To: Powers, Liam (POL)
Subject: TRF-11
Date: Wednesday, May 31, 2023 1:40:59 PM
Attachments: TRF-11 Automatic License Plate Recognition DRAFT 2023 (1) (1).docx

---

Sgt. Christopher Condlin #2970
Strategic Planning and Analysis Section
Office of the Superintendent
508-988-7439

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: Salvatore, Justin (POL)
To: Mellor, Jessica (POL)
Subject: Vigilant ALPR Training Materials
Date: Tuesday, September 26, 2023 9:22:01 PM
Attachments: AAMVA-LicensePlateReaderProgramBestPracticesGuide-October2021.pdf
Accessing Vigilant On-Demand Training.pdf
Adding New Hot Plates.pdf
Customizing QuickSearch View.pdf
Locate Analysis.pdf
LPR Class Roster-MSP-09142023.xlsx
MCCA-Automated-License-Plate-Reader-Technology-in-Law-Enforcement.pdf
My Profile - Configuring Alert Management (1).pdf
Open Source Free Internet Sites.xlsx
Open Source-Online Resources.pdf
Stakeout.pdf
Vigilant PlateSearch Active Hit Protocol Guidelines (1).pdf
Vigilant Training Team.pdf
Wild Card Help.pdf

Jess,

Attached are all of the training documents we received from the Vigilant (Motorola) ALPR trainer. Some are guides to the Vigilant system and others are just ALPR related background information.

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: Christopher Scandole
Subject: Vigilant LPR Follow Up
Date: Friday, September 15, 2023 5:45:43 AM
Attachments: Adding New Hot Plates.pdf
Accessing Vigilant On-Demand Training.pdf
Customizing QuickSearch View.pdf
Locate Analysis.pdf
Open Source Free Internet Sites.xlsx
My Profile - Configuring Alert Management (1).pdf
Open Source-Online Resources.pdf
Vigilant Training Team.pdf
Vigilant PlateSearch Active Hit Protocol Guidelines (1).pdf
Stakeout.pdf
Wild Card Help.pdf
AAMVA-LicensePlateReaderProgramBestPracticesGuide-October2021.pdf
MCCA-Automated-License-Plate-Reader-Technology-in-Law-Enforcement.pdf
LPR Class Roster-MSP-09142023.xlsx

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

Good Morning All,

It was an absolute pleasure meeting you all at the training session yesterday, and truly a privilege and honor to spend some time in the Bay State, among active members of the Massachusetts State Police. See the attachments to this email for some quick help references and free internet resources, to assist in your searches. The class roster is also attached, we encourage you to network with each other.

The below links are for our training site and for the On-Demand training.

https://vslea.org/

https://vigilant.policeoneacademy.com/login/#login

For Info on Commercial scans and for Certified Copies of Search results for court, send an email to VigilantRecords@MotorolaSolutions.com

For Case Assistance send an email to VigilantTraining@MotorolaSolutions.com

To request access to EPIC use this link - https://esp.usdoj.gov/nur/

Please feel free to reach out to the training team with any questions, and as always please stay safe and be careful out there

Chris

Chris Scandole
Manager, Customer Training & Development
Detective 1st Grade, NYPD (Retired)
Video Security & Analytics
Vigilant

m: +1.917.913 3351

Training: **www.vslea.org**

Case Assistance: **VigilantTraining@motorolasolutions.com**

CLICK HERE TO SCHEDULE AGENCY MANAGER TRAINING

CLICK HERE TO SCHEDULE END-USER TRAINING

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

Commonwealth Fusion Center

Watch Center – Work Flow Guide

DRAFT

License Plate Readers (LPRs)

DRAFT

Vigilant LPR Reader

Vigilant is an LPR reader utilized by many departments; however, the CFC receives information only from Lynn and Chelsea.

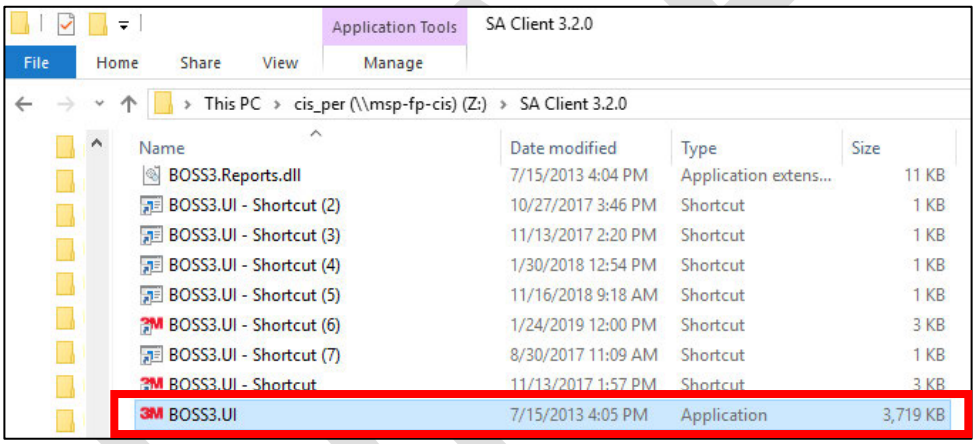
- Refer to Section 2: Accounts – Databases & Systems for log in information.

BOSS/3M LPR Reader

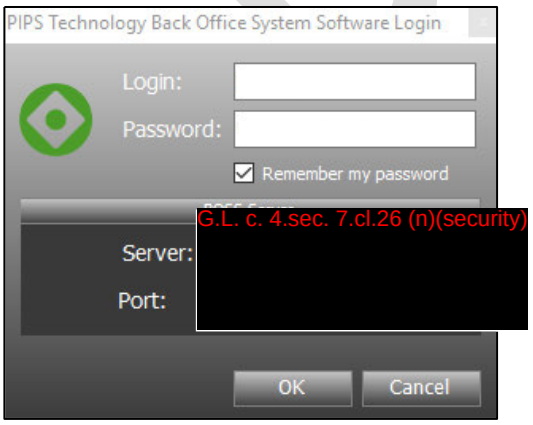
BOSS/3M is the primary LPR system utilized. The systems pulls information from LPRs controlled by MSP throughout the state.

1. **To install BOSS/3M on your computer, and add the shortcut, navigate to the "SA Client 3.2.0" on the M-Drive:** [redacted]

2. **Double click "BOSS3.IU" with "Application in the "Type" column to download the program**

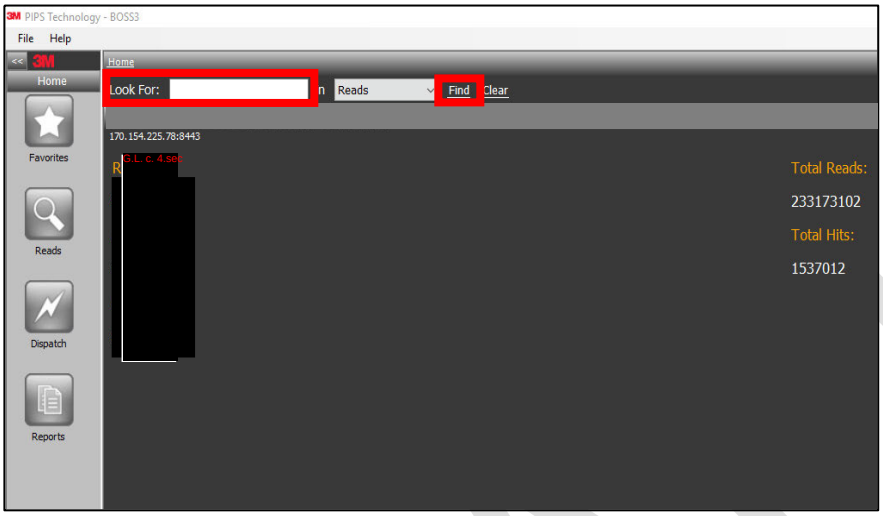


3. **Upon opening the program from your desktop, ensure the correct Server and Port are entered:**
   Server: 170.154.225.78 **Port:** 8443

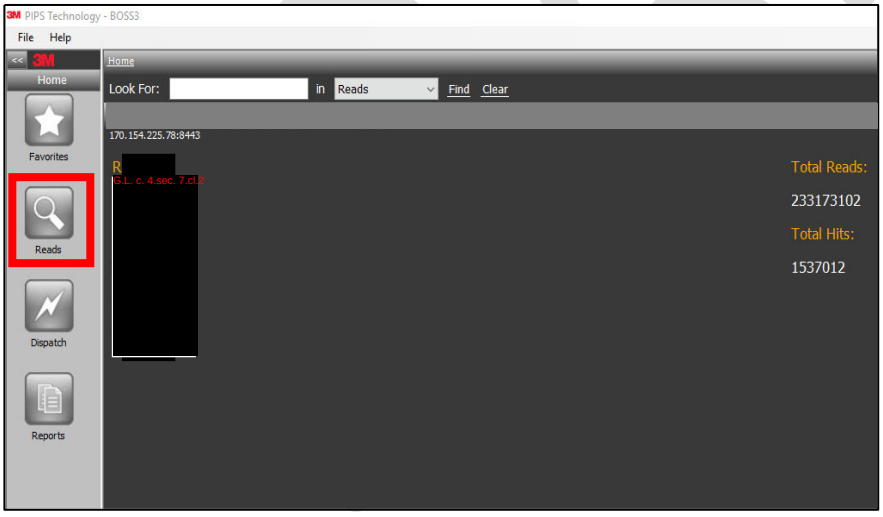


BOSS/3M LPR Reader - Searching a Plate

1. **Search a plate by typing the plate number into the “Look For:” box and clicking “Find”**



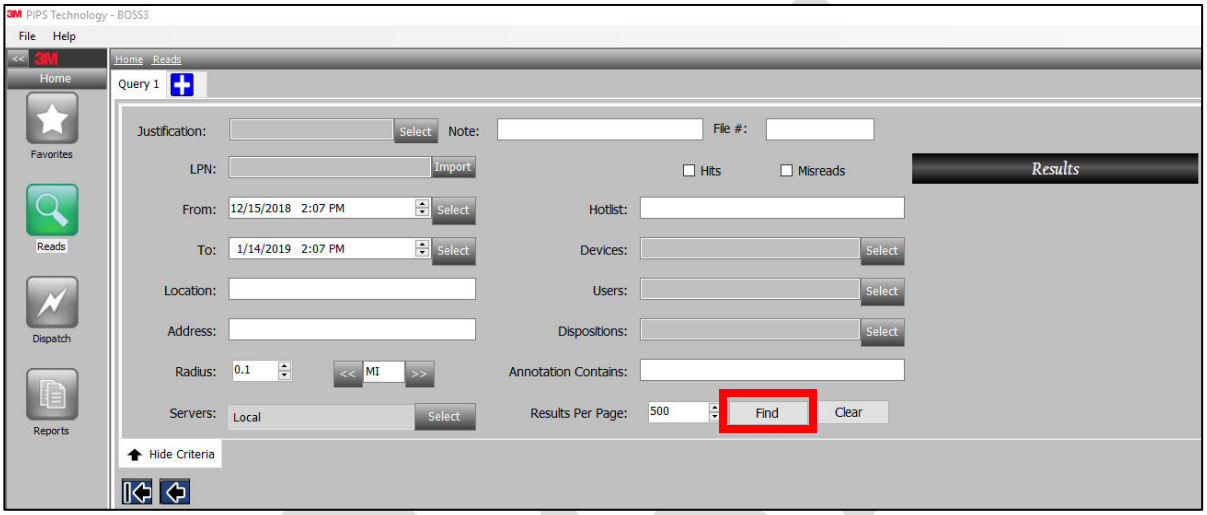
2. **Click “Reads” on the left tool bar to search a plate with more advanced parameters**



3. **The Reads page will display multiple search parameters, including:**
   - **Timeframe (dates and times)**
   - **Hotlist**
   - **LPR Device**
   - **Location**
   - **Address**
   - **Radius**

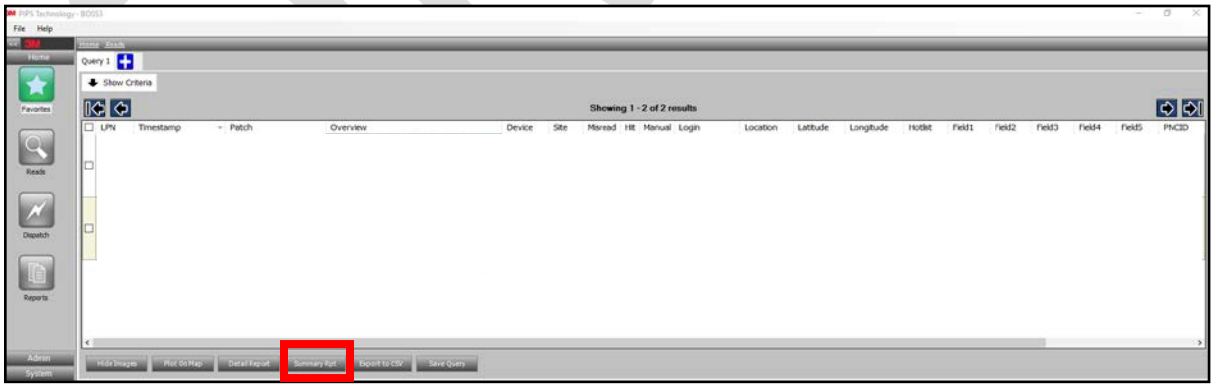
BOSS/3M LPR Reader - Searching a Plate (cont.)

4. **The Reads page will allow for multiple search parameters at once**
   - **Enter the plate number in "LPN"**
   - **Enter the appropriate parameters**
   - **Click "Find"**



BOSS/3M LPR Reader - Printing Results

1. **On the results page click "Summary Rpt" on the bottom tool bar**



2. **A popup will appear, click "All Results" or "Current Page" then select "OK"**

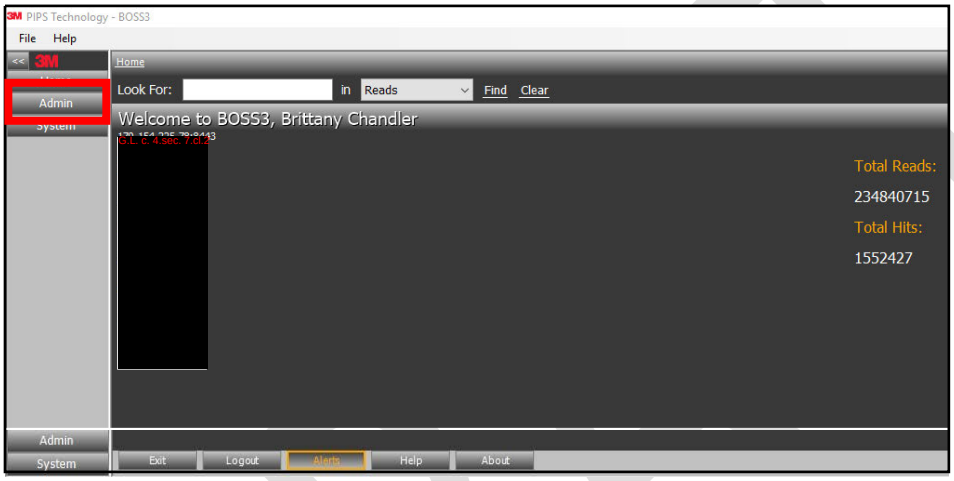
3. **Once the report loads, click the printer icon along the top tool bar**

Creating an LPR Hotlist

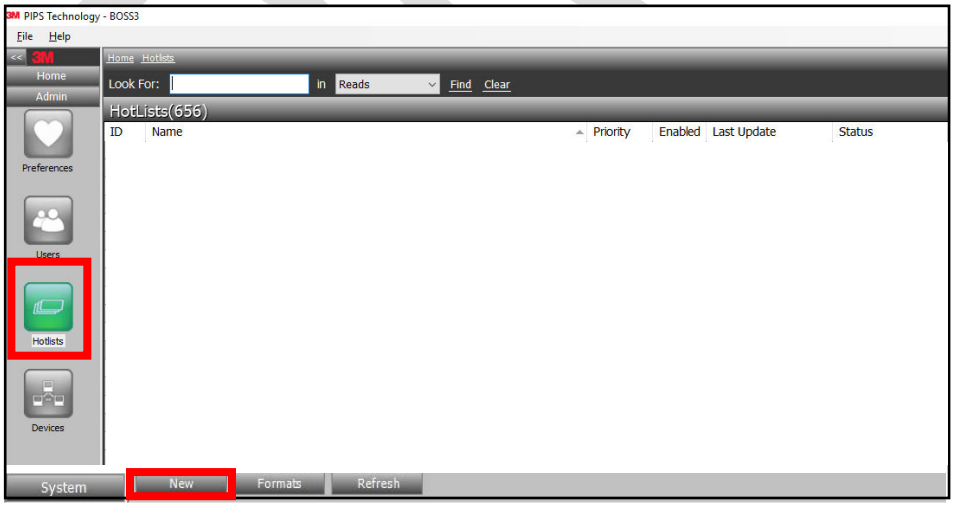
License plates of interest can be added to a Hotlist. When a Hotlist plate is read by an ALPR camera, an email will be sent to the requesting officer.

There are Two Steps to a Hotlist: Creating an LPR Hotlist and then Adding License Plates into an LPR Hotlist.

1. **From the main page, click "Admin" on the bottom of the left tool bar**

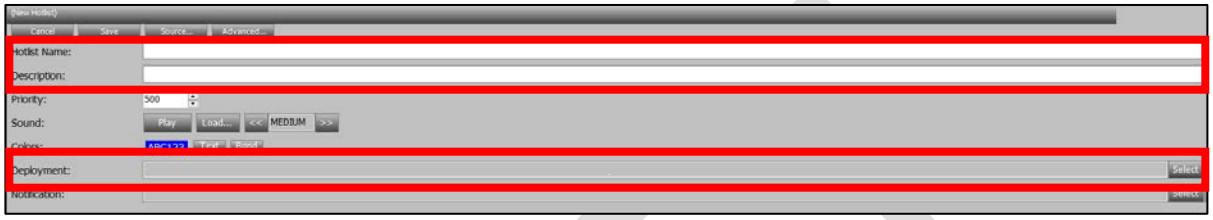


2. **The tool bars on the left and bottom will change, click "Hotlists" on the left toolbar then click "New" on the bottom tool bar**

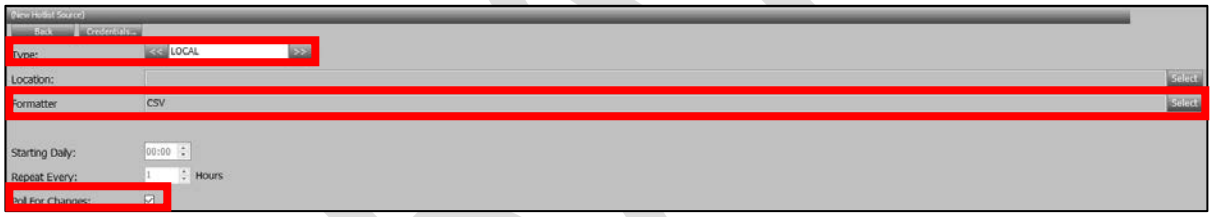


Creating an LPR Hotlist (cont.)

3. **In the "New Hotlist" box enter the following:**
   - **Hotlist Name: Agency – Officer – Case Number**
   - **Description: Officer name – Contact Information**
   - **Deployment: Click "Select" and check ALL boxes, then click "Save"**



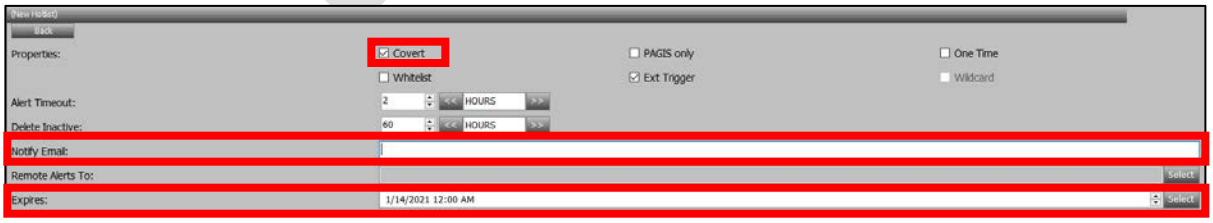
4. **Click "Source" and enter the following:**
   - **Type: Local (default)**
   - **Formatter: Select "Select" and select "CSV," then select "Save"**
   - **Poll for Changes: Check the box**



****Note: If not mentioned above, do not change****

5. **Click "Back"**

6. **Click "Advanced" and enter the following:**
   - **Covert: Check the box (Checking the box to ensures that passing ALPRs are NOT alerted)**
   - **Notify Email: Enter emails separated by commas with NO SPACES (Enter the Fusion Mailbox email with the requestor's email)**
   - **Expires: Three months from entry date**



****NOTE: Some requestors prefer text notifications, if so, follow the below steps****

DRAFT

Creating an LPR Hotlist (cont.)

Ask the requestor for their phone carrier information for the number they wish to receive text notifications
- In the "Notify Email" field enter the cellular number followed by @ and the corresponding cellular carrier suffix:

Mobile Carrier	SMS Gateway Domain
Alltel	sms.alltelwireless.com
AT&T	txt.att.net
Boost Mobile	sms.myboostmobile.com
Cricket Wireless	sms.mycricket.com
MetroPCS	mymetropcs.com
Project Fi	msg.fi.google.com
Republic Wireless	text.republicwireless.com
Sprint	messaging.sprintpcs.com
T-Mobile	tmomail.net
U.S. Cellular	email.uscc.net
Verizon Wireless	vtext.com
Virgin Mobile	vmobl.com

Example: 5088202233@vtext.com

7. **Click "Back"**

8. **Click "Save" then click "Save" again**

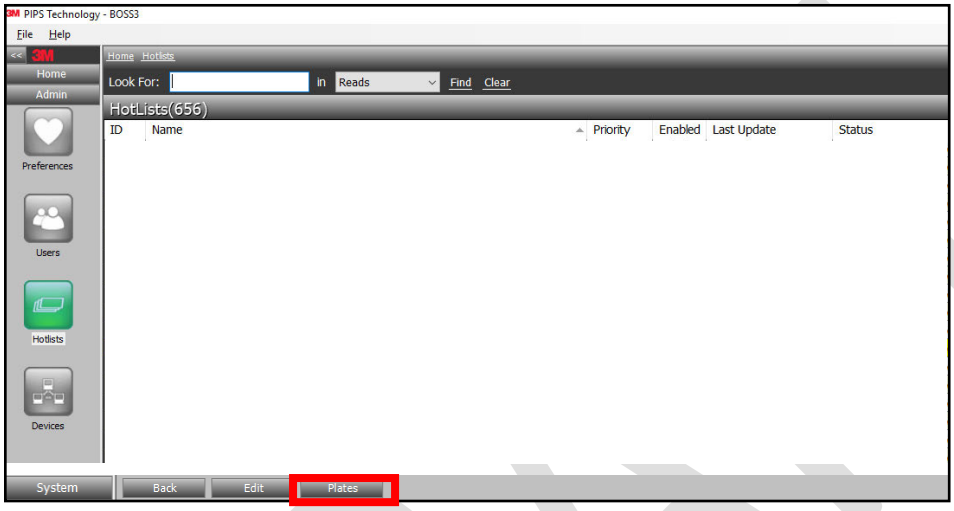
9. **Click "Yes" on the "Source File Name" error message**

DRAFT

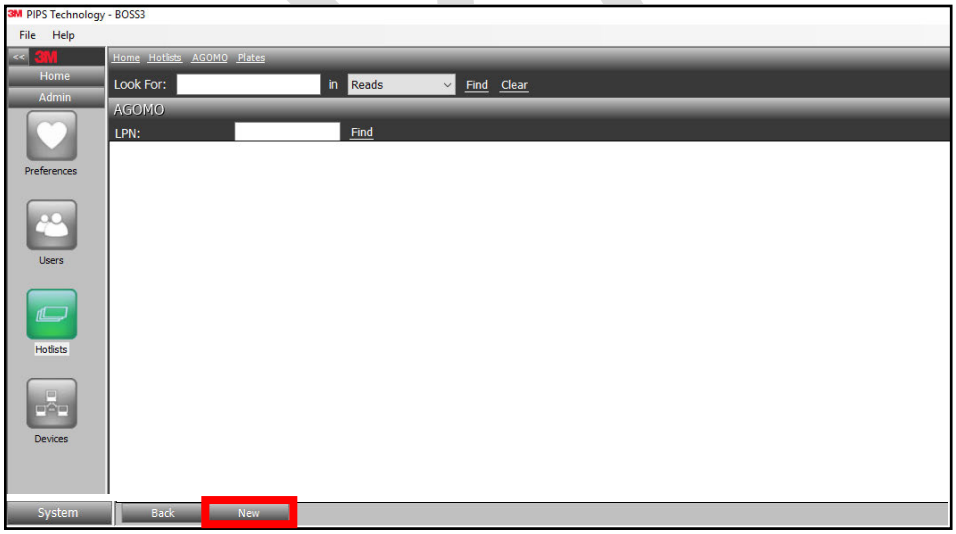
Adding a License Plate to an LPR Hotlist

1. **In the "Hotlist" section (Refer to Steps 1 and 2 above) click the appropriate Hotlist that needs a license plate added**

2. **Click "Plates" on the bottom tool bar**

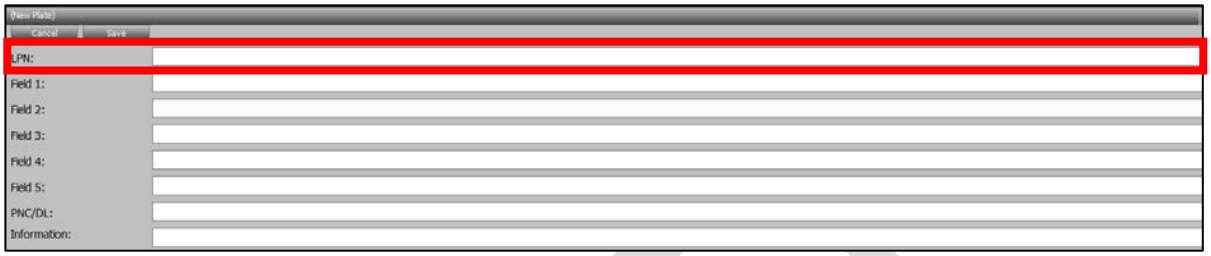


3. **Click "New" on the bottom tool bar**

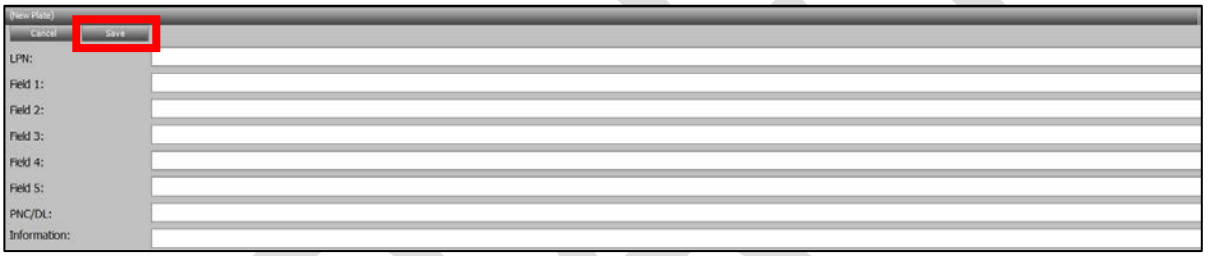


Adding a License Plate to an LPR Hotlist (cont.)

4. **Enter the following:**
   - LPN: Plate number (number only, do NOT add the state)



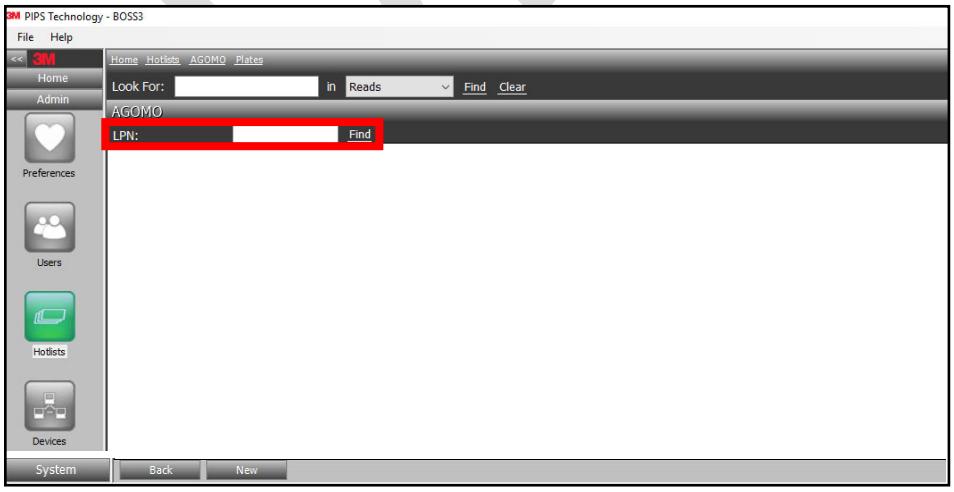
5. **Click "Save"**



Searching a License Plate in an LPR Hotlist

1. **In the LPR Hotlist navigate to the "Plates" section (Refer to Steps 1 and 2 above)**

2. **In the "LPN" field, enter the plate number of interest or % to see ALL plates on the Hotlist then select "Find"**



QRG

HSIN Quick Reference Guide

HSIN Exchange: Request For Information (RFI) Notifications

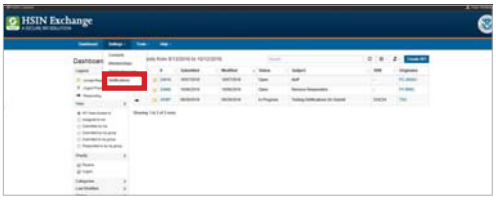
HSIN Exchange provides a tracking capability that will help fusion centers address requests for information (RFI) in a more efficient manner while providing quantitative metrics to assess and enhance their own operations. This quick reference guide provides an overview of how members can access and modify their notification settings. For additional information on HSIN Exchange, contact HSIN Outreach at HSIN.Outreach@hq.dhs.gov.

How to Access and Modify Notifications

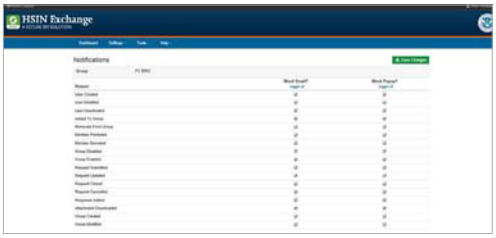
1. Navigate to HSIN Exchange (https://rfi.dhs.gov).
2. Click the **Settings** tab



3. Select **Notifications**

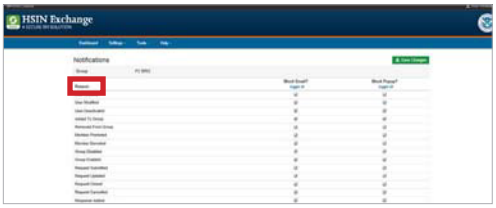


4. The Notifications page opens.

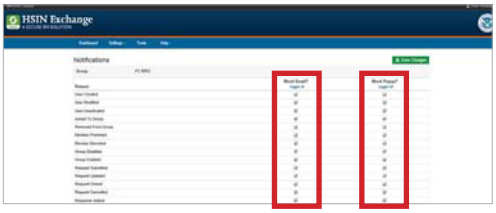


Note: There are 17 notifications that the system can send to a user. All notifications are sent by default to the user's email and through the browser if the user has an active session open.

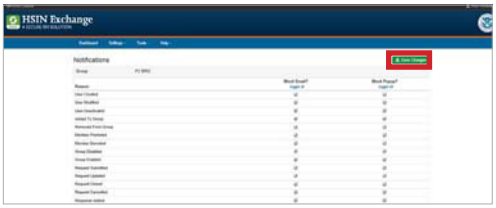
5. Identify the notification setting (reason) you wish to update.



6. For notification settings (reason) you want sent via email or browser, check the appropriate box. For notifications settings (reason) you do not want sent via email or browser, deselect the appropriate box.



7. After making any desired changes, click **Save Changes**.



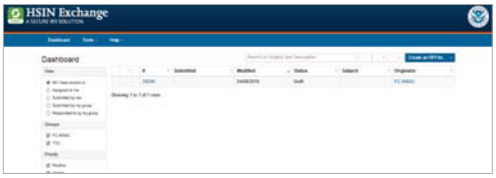
MEMBERS

HSIN Quick Reference Guide

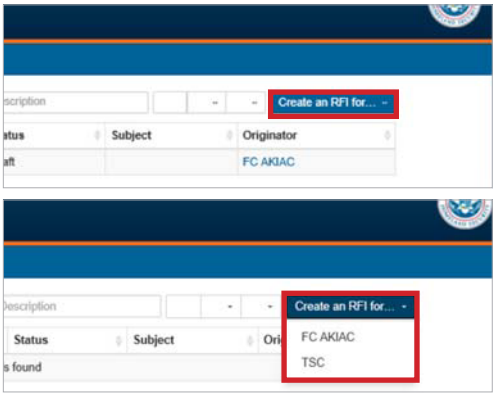
HSIN Exchange: How to Create and Submit an RFI

HSIN Exchange provides a tracking capability that will help fusion centers address requests for information (RFI) in a more efficient manner while providing quantitative metrics to assess and enhance their own operations. This quick reference guide provides an overview of how members can create and submit an RFI. For additional information on HSIN Exchange, contact HSIN Outreach at HSIN.Outreach@hq.dhs.gov.

1. Navigate to HSIN Exchange (https://rfi.dhs.gov).

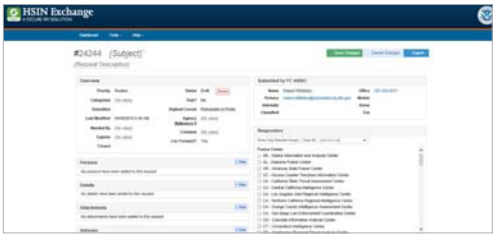


2. Click the **Create an RFI for** button.



Note: If you are a member of multiple groups, select the desired group to create a RFI.

3. The RFI form appears.



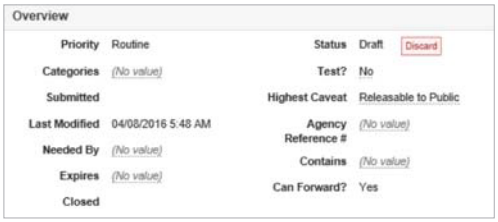
Note: Different group types will have different forms. This QRG is using the Fusion Center RFI form.

4. **Subject and Description:** The subject is the RFI title that is displayed in the dashboard. The description field allows members to describe the nature of their RFI.



Note: Click "Subject" or "Request Description" to enter text.

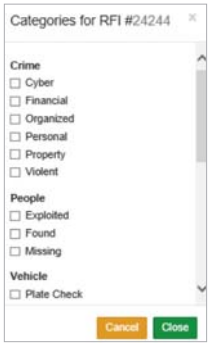
5. **Overview:** The overview section provides key information about the RFI.



A member is able to populate information on:

a. **Priority** – A dropdown selection. Requestors may select from "Routine" or "Urgent".

b. **Categories** – A multi-select pop-up and will vary by group. To select a category, click into **No Value**. A pop-up window appears with the different categories.



c. **Submitted** – This field automatically populates based on when the RFI was submitted.

d. **Last modified** –This field automatically populates based on when the RFI was last modified.

e. **Needed By** – The date and time a response is required by.

f. **Expires** – The RFI can be set to automatically expire at a certain date and time. An RFI will close at 12 midnight on the expiration date.

g. **Closed** – This field automatically populates based on when the RFI was closed.

h. **Status** – The current status of the RFI. This can be either Draft, Open, In Progress, Canceled, Closed or Expired. If a member initiates an RFI but wants to delete it prior to submission, click the **Discard** button.

i. **Highest Caveat** – The highest level of data contained in the RFI. This can be either Releasable to Public, FOUO or LES.

j. **Agency/Case Reference #** – Free text field to allow a user to attach an agency case number to the RFI.

k. **Contains** – Checkboxes for USPER and LES attributes.

l. **Can Forward** – A "yes" or "no" selection lets recipients know whether they can or cannot send the RFI to another group.

6. **Persons:** The persons section allows user to enter specifics and/or comments related to a person(s) related to the request.



Note: The New button, or any Add button, indicates that you can add as many items as needed for a particular section.

7. **Details:** The details section allows users to enter specifics and/or comments related to the RFI.



Note: The New button, or any Add button, indicates that you can add as many items as needed for a particular section.

8. **Attachments:** Members can attached any document type. Recommended file size is up to 16MB.



9. **Vehicles:** The section allows users to enter specifics and/or comments related to a vehicle(s).

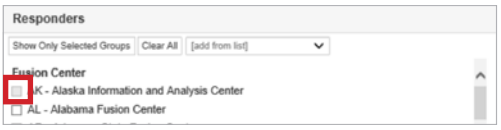


10. **Submitted by:** Automatically provides the requestor's contact information and group affiliation. Members can update their information via the contact card.

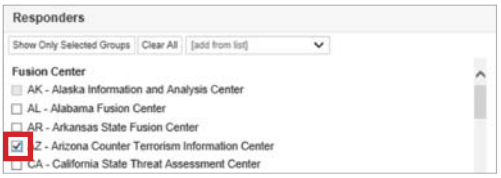


11. **Responders:** The responders section allows members to select groups the RFI should be sent to.

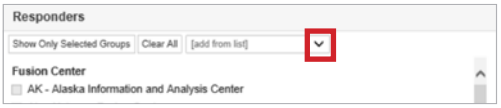
a. To select group(s) that the RFI will be sent to, click the **Checkbox** next to the group name.



b. To remove group(s) from a request, click a **Marked Checkbox**.



c. To add groups from a distribution list, click the **Drop Arrow**.



12. Once the form is populated, click **Submit** located in the Overview section.



13. A HSIN Exchange Request message is sent to group members with the **Request Submitted** notifications feature enabled.



MEMBERS

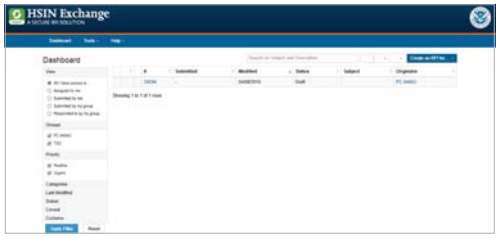
QRG

HSIN Quick Reference Guide

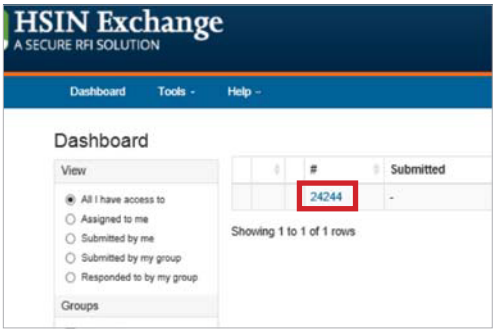
HSIN Exchange: How to Respond to an RFI

HSIN Exchange provides a tracking capability that will help fusion centers address requests for information (RFI) in a more efficient manner while providing quantitative metrics to assess and enhance their own operations. This quick reference guide provides an overview of how members can respond to an RFI. For additional information on HSIN Exchange, contact HSIN Outreach at HSIN.Outreach@hq.dhs.gov.

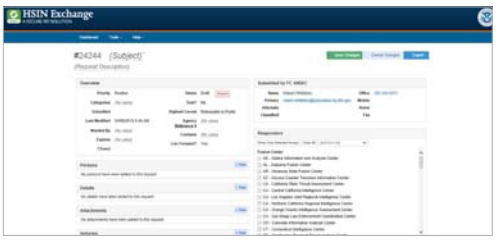
1. Navigate to HSIN Exchange (https://rfi.dhs.gov).



2. Click the **number** under the pound sign column. This number is automatically assigned to an RFI when it's created.



3. The RFI appears.



4. Find your designated group. Click **Respond**.



Note: If the responder has not responded to the RFI, this section will state "No responses."

5. Enter your response and add any attachments, then click **Submit Response**.



Note: Recommended file size is up to 16MB.

6. The new response appears.



MEMBERS

QRG

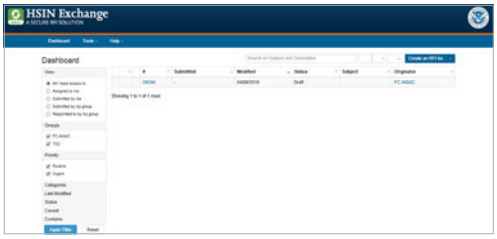
HSIN Quick Reference Guide

HSIN Exchange: How to Close an RFI and End an RFI Response Conversation

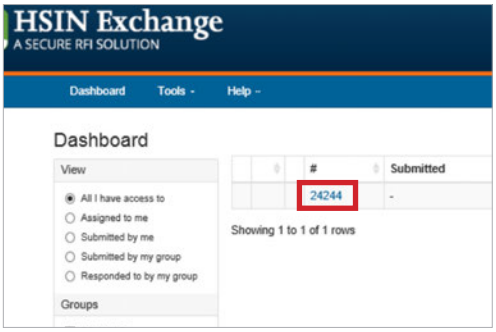
HSIN Exchange provides a tracking capability that will help fusion centers address requests for information (RFI) in a more efficient manner while providing quantitative metrics to assess and enhance their own operations. This quick reference guide provides an overview of how members can close an RFI and manage RFI response conversation strings as members of an originating group. For additional information on HSIN Exchange, contact HSIN Outreach at HSIN.Outreach@hq.dhs.gov.

Close an RFI

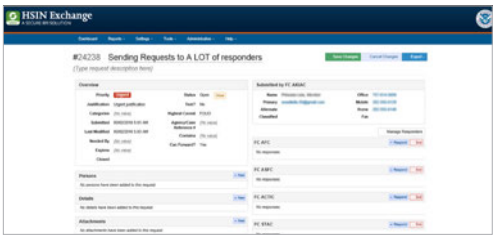
1. Navigate to HSIN Exchange (https://rfi.dhs.gov).



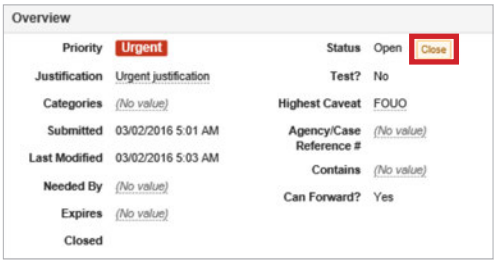
2. Click the **number** under the pound sign column. This number is automatically assigned to an RFI when it's created.



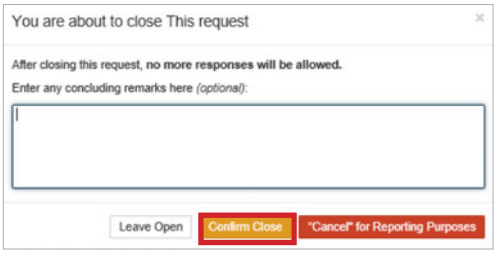
3. The RFI appears.



4. Under the Overview section, click **Close**.



5. Enter any concluding remarks. Click **Confirm Close**.

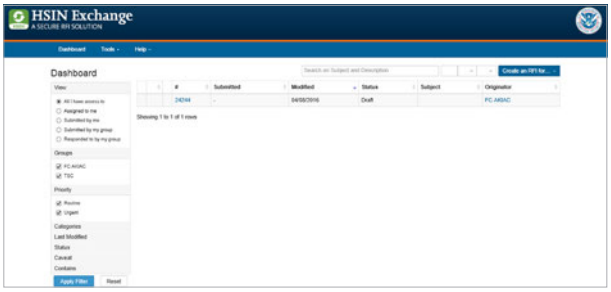


6. The RFI is now closed.

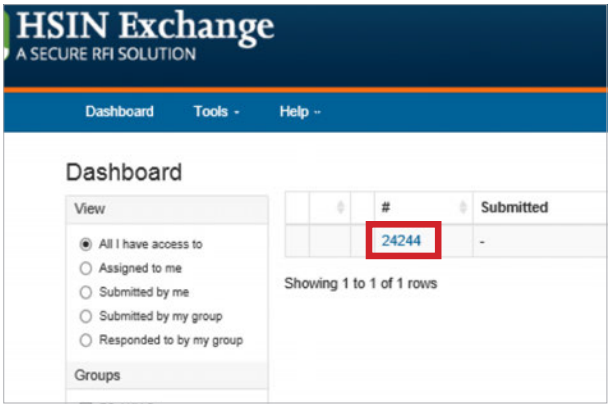
End an RFI Response(s)

Note: Only members of the originating agency can end a response.

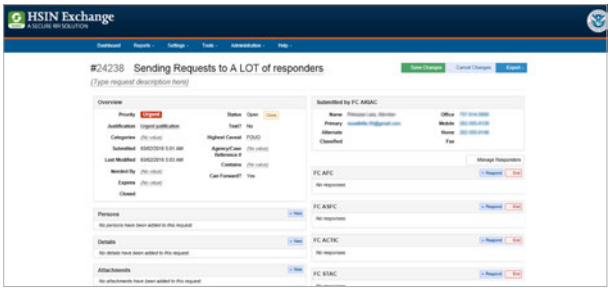
1. Navigate to HSIN Exchange (https://rfi.dhs.gov).



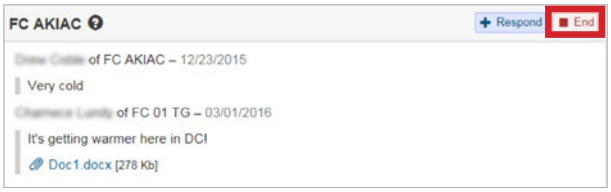
2. Click the **number** under the pound sign column.



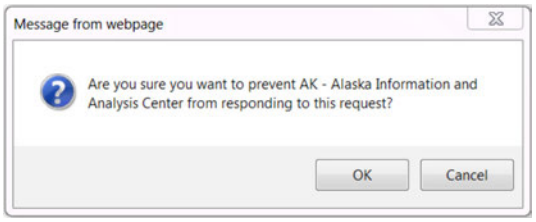
3. The RFI appears.



4. Under **Manage Responders**, select your designated group and click **End**.



5. When prompted with "Are you sure you want to prevent…from responding to this request?" Click **OK**.



6. The conversation has ended.

FACT SHEET

HSIN-Intel Homeland Security Information Network Intelligence

Homeland Security Information Network-Intelligence (HSIN-Intel)

HSIN-Intel is a secure community that connects Federal, State, Local, Territorial and Tribal partners and promotes the exchange and analysis of controlled, unclassified intelligence and threat related information.



HSIN-Intel Purpose

- Foster community and coordination between fusion centers and homeland security partners across the nation
- Disseminate timely intelligence derived from SLTT, DHS, Federal partners and the Intelligence Community
- Exchange of raw information during national or regional incidents
- Provide a secure, single-access point to unclassified intelligence data which authorized stakeholders may access from anywhere at any time

HSIN-Intel Member Benefits

- Access to the national network of fusion centers analysts and intelligence professionals
- Access to sensitive "For Official Use Only" (FOUO) and Law Enforcement Sensitive (LES) shared by Fusion Centers, DHS, and other Federal Partners
- 24/7 situational awareness tools to ensure awareness and coordination during regional and national level incidents
- Ability to respond promptly to state and local partner requests for information

Minimum Eligibility Requirements

1. **Be a U.S. Citizen**
2. **Be a full-time, current employee of a law enforcement, criminal justice, intelligence, or homeland security government agency**
3. **Directly support information and intelligence analysis, sharing, or collection activities**
4. **Be associated with a fusion center, as verified by the fusion center, or other centralized intelligence capability (i.e. RISS center, HIDTA, EPIC, NORTHCOM, etc.) recognized by the HSIN-Intel Program Office**
5. **Have a government email address**

Governance

HSIN-Intel is governed by the HSIN Working Group, which is comprised of fusion center professionals represeting the four National Network of Fusion Center regions. Visit HSIN-Intel to view the HSIN-Intel Charter and see the current list of Working Group members representing your region. For more information about the Working Group, contact HSIN-Intel at HSIN.Intel.PMO@hq.dhs.gov.



uest Access to HSIN-Intel

To request access, please email your name, affiliated organization, email address and phone number, and a short justification to HSIN.Intel.PMO@hq.dhs.gov.

For more information, contact HSIN-Intel at HSIN.Intel.PMO@hq.dhs.gov or visit our website at https://hsin.dhs.gov/collab/intel.

Scan the QR code* or visit our website to learn more about how HSIN can help support your mission.

* You must have a QR code reader installed on your mobile device.

Update the HSIN Connect Display Name in HSIN Connect Meeting Room

QRG

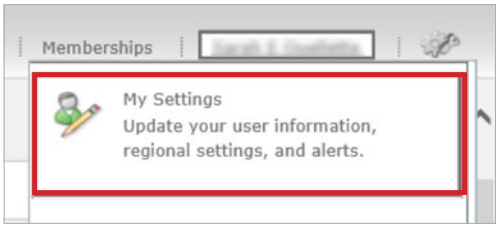
Use this quick reference guide to learn how to update your display name in a HSIN Connect meeting room. The first exercise will be performed by all users, and the second will be performed by the meeting host.

1. The first exercise describes the steps to change your HSIN Connect display name. Users must create their HSIN Connect display name through their HSIN user profile. Once the name has been created or modified, it will take up to 24 hours for the name to update in the HSIN Connect meeting room.
2. The second exercise describes the next steps for the Meeting Host to modify preferences to share the updated display name in the HSIN Connect meeting room.

Once the HSIN Connect meeting room is updated, the HSIN Connect display name will appear in the Attendees pod. If the user chooses not create a HSIN Connect display name, the default will be the user's first name, last name. If the meeting Host changes the HSIN Connect display name during the meeting, the Chat pod will only reflect the changes going forward and the past chat history will not be changed.

Create a HSIN Connect Display Name in the User Profile

1. Navigate to HSIN Central https://hsin.dhs.gov
2. From the Universal Navigation bar, click **Your Name** and select **My Settings**



3. The User Profile page appears, click **Edit Profile**



4. Scroll down to the **HSIN Connect Display Name** section and enter the desired name



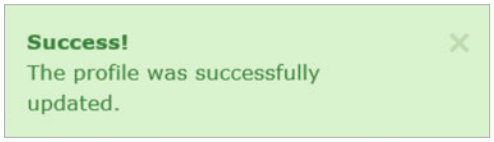
Note: HSIN-Intel Users must include your organization name before your first and last name (examples below):

- **State and local SitRoom members:** Enter your state abbreviation, your fusion center acronym and your first and last name (e.g., CA JRIC John Doe)
- **Federal agency SitRoom members:** Enter your agency acronym, your office acronym, and your first and last name (e.g., DHS I&A Jane Doe)

5. Click **Save** to save the change to the profile



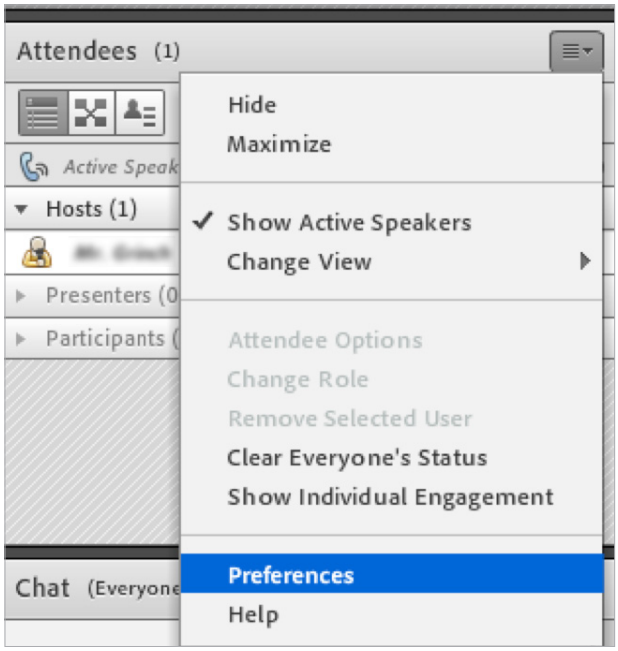
6. A confirmation message will appear



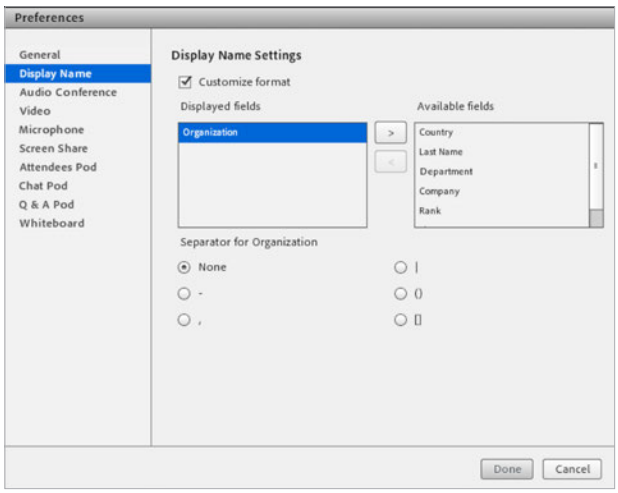
Display the HSIN Connect Display Name in a HSIN Connect Meeting Room

Note: The following exercise is to be performed by the Meeting Host.

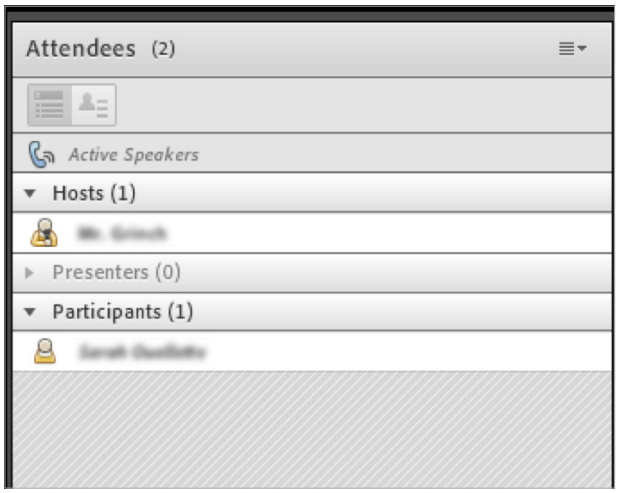
1. Open a HSIN Connect meeting room as a Host
2. Click the **Attendees pod** to view the drop down menu, then select **Preferences**



3. Click **Display Name** and check the **Customize format** checkbox. Remove the 'First Name' and 'Last Name' fields from appearing under the Displayed fields, and then add the 'Organization' field to the Displayed fields.



4. Click **Done** to save the changes and view the HSIN Connect Display Name in the Attendees pod



FACT SHEET

National Situational Awareness Room (SitRoom)



The National Situational Awareness Room (SitRoom) is a collaboration tool and source for real-time information and intelligence sharing between fusion centers and homeland security partners concerning events and incidents having a regional or national-level impact.

Eligibility Requirements

Eligibility requirements mirror HSIN-Intel membership, as outlined in the HSIN-Intel charter, and are provided in accordance with the *Standard Operating Procedure on Nomination, Validation, and Access to HSIN-Intel*, and the *Standard Operating Procedure for the National Situational Awareness Room*.

- An active HSIN-Intel membership is a prerequisite, but is not the sole qualifying factor for access.
  - Be a U.S. citizen
  - Be a full-time, current employee of a law enforcement, criminal justice, intelligence, or homeland security government agency
  - Directly support information and intelligence analysis, sharing, or collection activities
  - Be associated with a fusion center, as verified by the fusion center, or other centralized intelligence capability (i.e. RISS Center, HIDTA, EPIC, NORTHCOM, etc.) recognized by the HSIN-Intel Program Management Office (PMO)
  - Maintain a government email address
- Access to SitRoom must be approved by the Fusion Center HSIN-Intel Coordinator in your area of responsibility (AOR).
- Federal personnel in the National Capital Region and those that support national-level missions (i.e., EPIC, NORTHCOM, etc.) may coordinate with HSIN-Intel PMO for access.
- Complete the required SitRoom 101 training hosted on the HSIN Learning Management System (HSIN Learn) at https://learn.dhs.gov/sitroom101/ *(All users must be approved members of HSIN-Intel to access the SitRoom 101 training).*

SitRoom Purpose

- Collaborate in advance of, during, and/or after a critical incident that has a regional or national-level impact, and where timely and accurate information is essential to maintain situational awareness and/or facilitate mitigation and response efforts
- Facilitate real-time, and often raw or unvetted, information and intelligence sharing between fusion centers during critical incidents – primarily via the AOR directly impacted by the incident
- During a critical incident, any shared information is owned and controlled by the lead fusion center or its designee
- Afford a secure, single-access point to sensitive but unclassified information, which authorized users may access from anywhere, at any time
- Active and operational twenty-four hours a day, seven days a week

Approved users can access SitRoom via the HSIN-Intel landing page or directly using the following link: https://share.dhs.gov/sitroom.

Please note that guest access is not authorized for SitRoom. Only vetted HSIN-Intel members that have been authorized for access and completed all required training are eligible to access SitRoom.



Request Access to SitRoom and/or HSIN-Intel

To request access to SitRoom and/or HSIN-Intel, contact the HSIN-Intel Coordinator located at the Fusion Center in your AOR, or email your name, affiliated organization, email address and phone number, and a short justification to HSIN.Intel.PMO@hq.dhs.gov.

For more information, contact HSIN-Intel at HSIN.Intel.PMO@hq.dhs.gov or visit our website at http://hsin.dhs.gov/collab/intel.

Search Warrant Process

Tim Ferriter, Deputy Captain, Search Warrant Team
Christa Elliott, Assistant District Attorney, Search Warrant Team

G.L.[1288] c. 276, § 1: Massachusetts Search Warrant Statute

“A court or justice authorized to issue warrants in criminal cases may, upon complaint on oath that the complainant believes that any of the property or articles hereinafter named are concealed in a house, place, vessel or vehicle or in the possession of a person anywhere within the commonwealth and territorial waters thereof, if satisfied that there is probable cause for such belief, issue a warrant identifying the property and naming or describing the person or place to be searched and commanding the person seeking such warrant to search for the following property or articles . . . “

What is Required?

Legal Sufficiency:

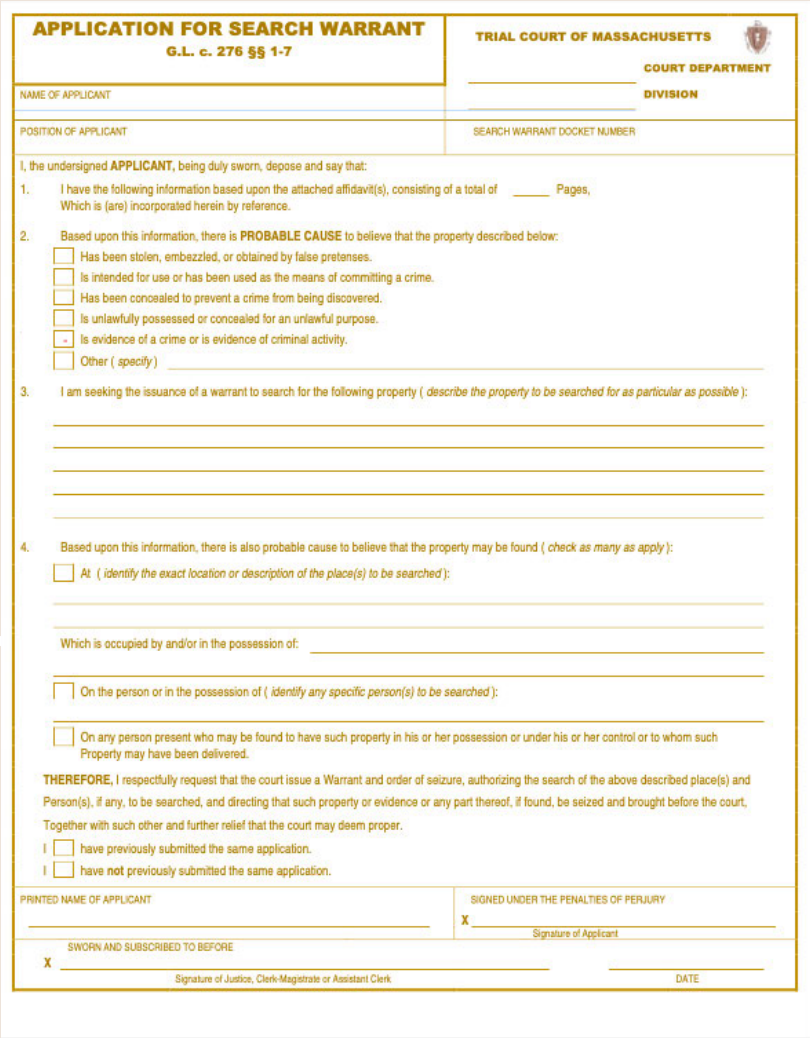
1. Probable Cause to believe a crime has been committed;
2. Probable Cause to believe evidence - described with particularity - of that crime will be found; and
3. Reasonable likelihood that specified items will be found in the place to be searched (Nexus).
4. ALWAYS CONSIDER STALENESS.

Parts of a Search Warrant:

1. Application
2. Affidavit
3. Search Warrant
4. Search Warrant Return

1290

Application



APPLICATION FOR SEARCH WARRANT
G.L. c. 276 §§ 1-7

TRIAL COURT OF MASSACHUSETTS
COURT DEPARTMENT
DIVISION

NAME OF APPLICANT

POSITION OF APPLICANT

SEARCH WARRANT DOCKET NUMBER

I, the undersigned **APPLICANT**, being duly sworn, depose and say that:

1. I have the following information based upon the attached affidavit(s), consisting of a total of _____ Pages, Which is (are) incorporated herein by reference.

2. Based upon this information, there is **PROBABLE CAUSE** to believe that the property described below:
   - ☐ Has been stolen, embezzled, or obtained by false pretenses.
   - ☐ Is intended for use or has been used as the means of committing a crime.
   - ☐ Has been concealed to prevent a crime from being discovered.
   - ☐ Is unlawfully possessed or concealed for an unlawful purpose.
   - ☐ Is evidence of a crime or is evidence of criminal activity.
   - ☐ Other (*specify*) _____

3. I am seeking the issuance of a warrant to search for the following property (*describe the property to be searched for as particular as possible*):

4. Based upon this information, there is also probable cause to believe that the property may be found (*check as many as apply*):
   - ☐ At (*identify the exact location or description of the place(s) to be searched*):
   - Which is occupied by and/or in the possession of: _____
   - ☐ On the person or in the possession of (*identify any specific person(s) to be searched*): _____
   - ☐ On any person present who may be found to have such property in his or her possession or under his or her control or to whom such Property may have been delivered.

THEREFORE, I respectfully request that the court issue a Warrant and order of seizure, authorizing the search of the above described place(s) and Person(s), if any, to be searched, and directing that such property or evidence or any part thereof, if found, be seized and brought before the court, Together with such other and further relief that the court may deem proper.

I ☐ have previously submitted the same application.
I ☐ have **not** previously submitted the same application.

PRINTED NAME OF APPLICANT

SIGNED UNDER THE PENALTIES OF PERJURY
X _____
Signature of Applicant

SWORN AND SUBSCRIBED TO BEFORE
X _____
Signature of Justice, Clerk-Magistrate or Assistant Clerk

DATE

Choosing a Court



District Court

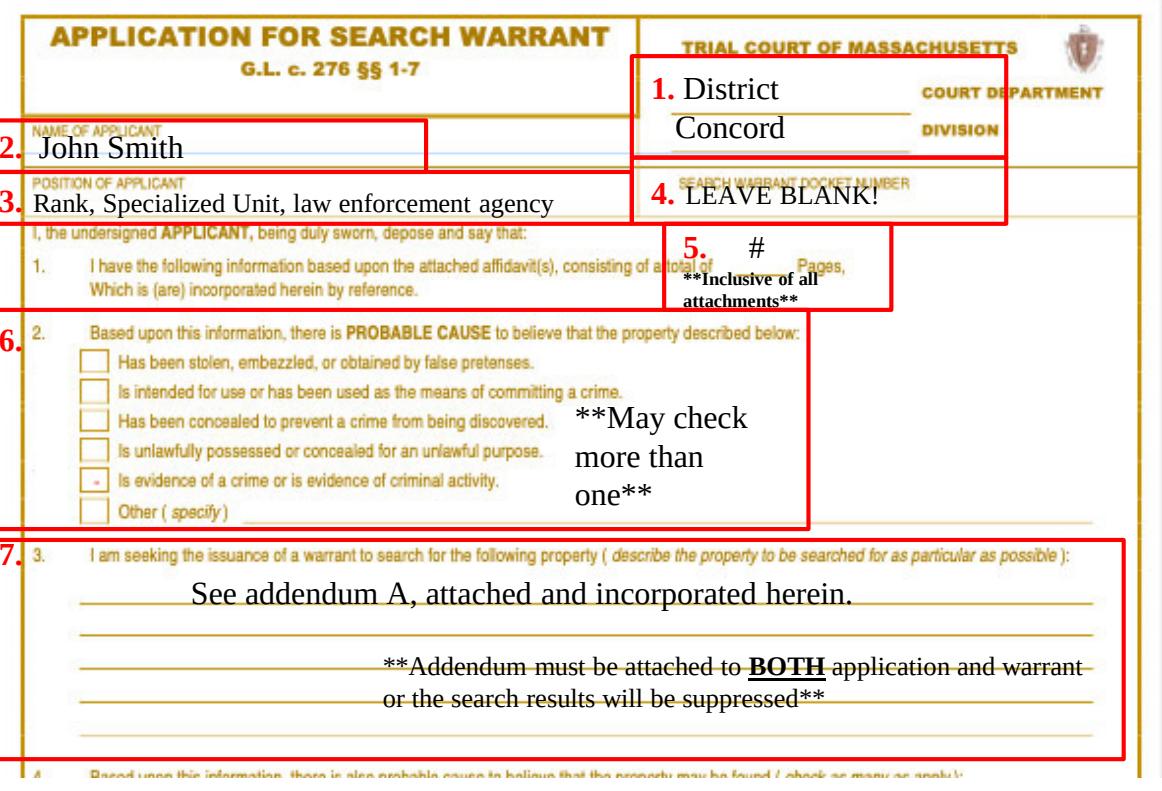
- You should seek a warrant from the court with jurisdiction over the crime



Superior Court has <u>exclusive</u> jurisdiction over:

- Wiretaps & Pen Registers
- Search warrant for emails of an indicted defendant
- Tower Dumps (NOT Geofence)

The Application Continued



APPLICATION FOR SEARCH WARRANT
G.L. c. 276 §§ 1-7

TRIAL COURT OF MASSACHUSETTS

1. District
Concord
COURT DEPARTMENT
DIVISION

NAME OF APPLICANT
2. John Smith

POSITION OF APPLICANT
3. Rank, Specialized Unit, law enforcement agency

SEARCH WARRANT DOCKET NUMBER
4. LEAVE BLANK!

I, the undersigned **APPLICANT**, being duly sworn, depose and say that:

1. I have the following information based upon the attached affidavit(s), consisting of a total of **5.** # Pages, Which is (are) incorporated herein by reference.

****Inclusive of all attachments****

6.

2. Based upon this information, there is **PROBABLE CAUSE** to believe that the property described below:
- ☐ Has been stolen, embezzled, or obtained by false pretenses.
- ☐ Is intended for use or has been used as the means of committing a crime.
- ☐ Has been concealed to prevent a crime from being discovered.
- ☐ Is unlawfully possessed or concealed for an unlawful purpose.
- ☒ Is evidence of a crime or is evidence of criminal activity.
- ☐ Other (*specify*)

****May check more than one****

7.

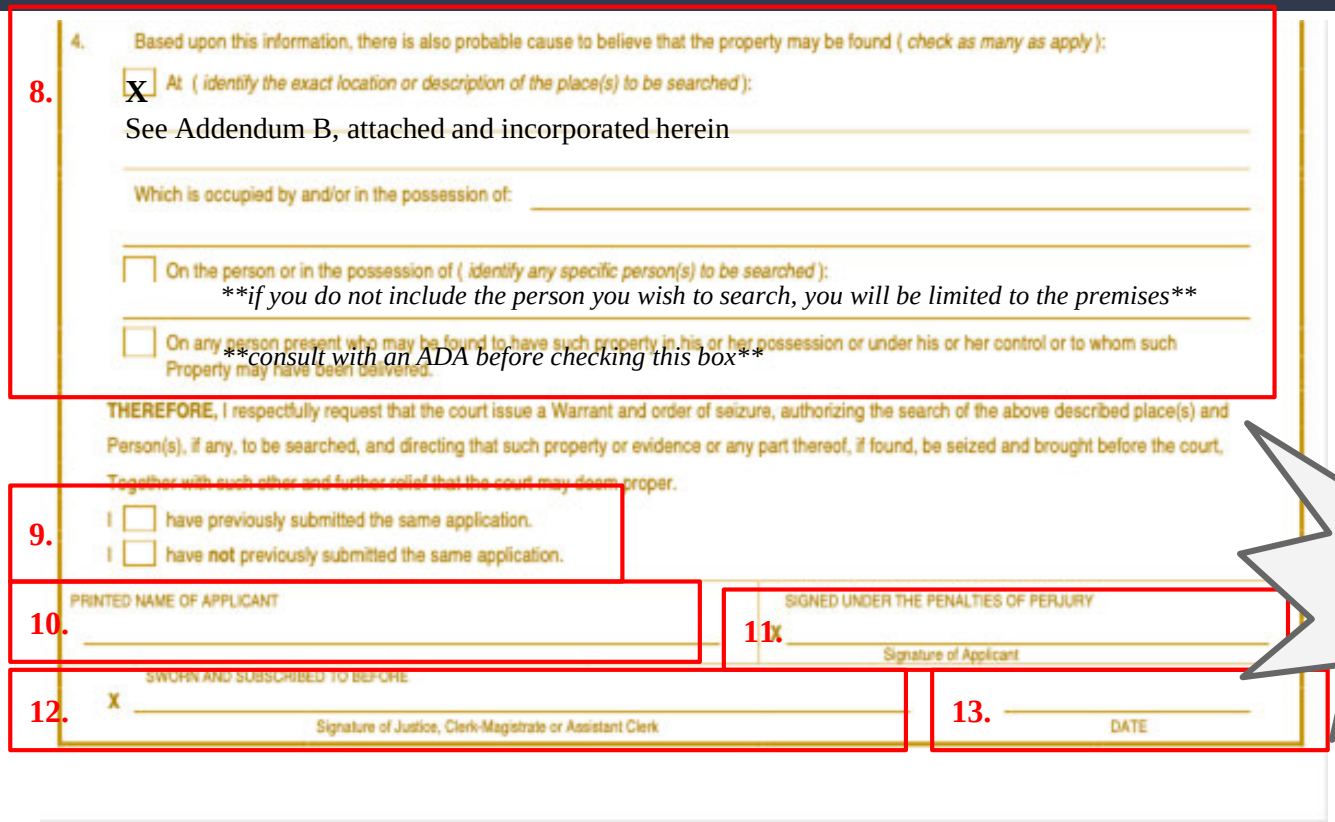
3. I am seeking the issuance of a warrant to search for the following property (*describe the property to be searched for as particular as possible*):

See addendum A, attached and incorporated herein.

****Addendum must be attached to BOTH application and warrant or the search results will be suppressed****

4. Based upon this information, there is also probable cause to believe that the property may be found (*check as many as apply*):

The Application Continued



4. Based upon this information, there is also probable cause to believe that the property may be found (*check as many as apply*):

8.

☒ At (*identify the exact location or description of the place(s) to be searched*):

See Addendum B, attached and incorporated herein

Which is occupied by and/or in the possession of:

☐ On the person or in the possession of (*identify any specific person(s) to be searched*):

if you do not include the person you wish to search, you will be limited to the premises

☐ On any person present who may be found to have such property in his or her possession or under his or her control or to whom such Property may have been delivered.

consult with an ADA before checking this box

THEREFORE, I respectfully request that the court issue a Warrant and order of seizure, authorizing the search of the above described place(s) and Person(s), if any, to be searched, and directing that such property or evidence or any part thereof, if found, be seized and brought before the court, Together with such other and further relief that the court may deem proper.

9.

I ☐ have previously submitted the same application.

I ☐ have **not** previously submitted the same application.

10. PRINTED NAME OF APPLICANT

11. SIGNED UNDER THE PENALTIES OF PERJURY

X _____ Signature of Applicant

12. SWORN AND SUBSCRIBED TO BEFORE

X _____ Signature of Justice, Clerk-Magistrate or Assistant Clerk

13. _____ DATE

Do not sign or date until you are before the clerk or judge.

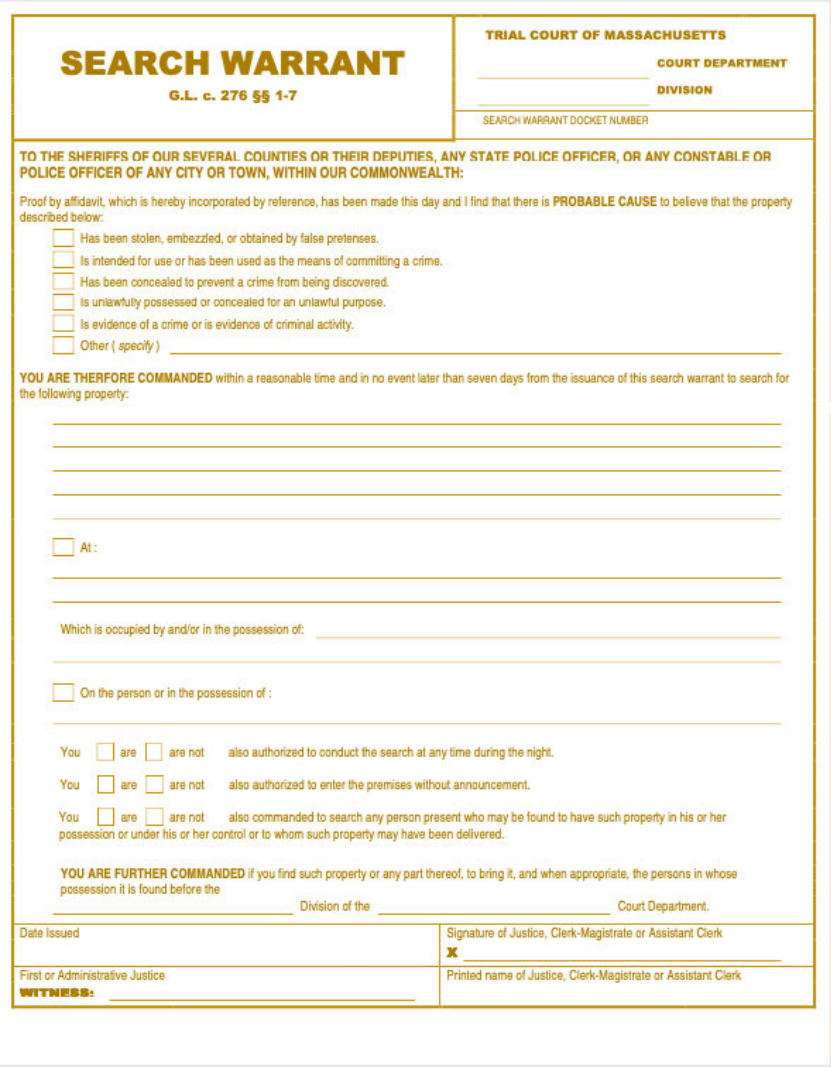
Out of State Warrants



- If applying for a warrant that will be executed outside Massachusetts:
  - Apply in the normal course in Massachusetts;
  - Contact the local PD and DA's office in the executing state; and
  - Follow their instructions on how to proceed.

The Warrant

Remember - whether using carbon copy or fillable pdf, much of the information from the application automatically transfers to the warrant itself.



SEARCH WARRANT

G.L. c. 276 §§ 1-7

TRIAL COURT OF MASSACHUSETTS

COURT DEPARTMENT

DIVISION

SEARCH WARRANT DOCKET NUMBER

TO THE SHERIFFS OF OUR SEVERAL COUNTIES OR THEIR DEPUTIES, ANY STATE POLICE OFFICER, OR ANY CONSTABLE OR POLICE OFFICER OF ANY CITY OR TOWN, WITHIN OUR COMMONWEALTH:

Proof by affidavit, which is hereby incorporated by reference, has been made this day and I find that there is **PROBABLE CAUSE** to believe that the property described below:

- ☐ Has been stolen, embezzled, or obtained by false pretenses.
- ☐ Is intended for use or has been used as the means of committing a crime.
- ☐ Has been concealed to prevent a crime from being discovered.
- ☐ Is unlawfully possessed or concealed for an unlawful purpose.
- ☐ Is evidence of a crime or is evidence of criminal activity.
- ☐ Other (*specify*) _____

YOU ARE THERFORE COMMANDED within a reasonable time and in no event later than seven days from the issuance of this search warrant to search for the following property:

_____

_____

_____

_____

_____

☐ At :

_____

_____

Which is occupied by and/or in the possession of: _____

_____

☐ On the person or in the possession of :

_____

You ☐ are ☐ are not also authorized to conduct the search at any time during the night.

You ☐ are ☐ are not also authorized to enter the premises without announcement.

You ☐ are ☐ are not also commanded to search any person present who may be found to have such property in his or her possession or under his or her control or to whom such property may have been delivered.

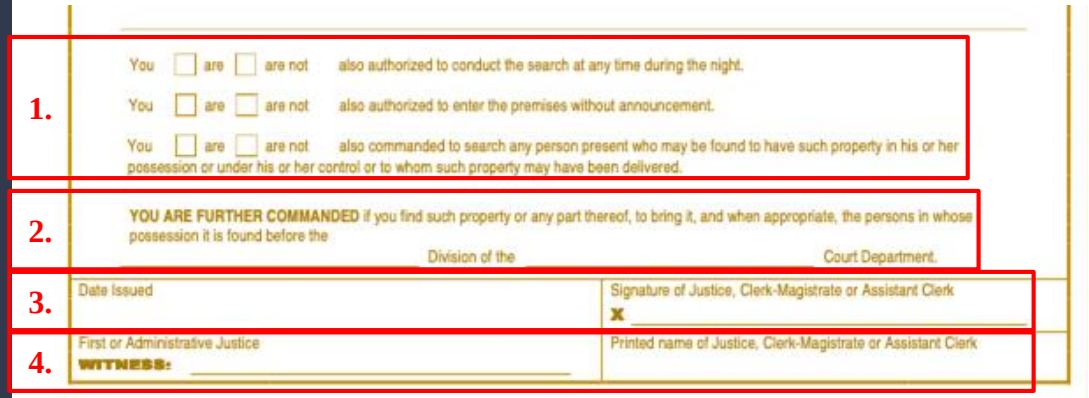
YOU ARE FURTHER COMMANDED if you find such property or any part thereof, to bring it, and when appropriate, the persons in whose possession it is found before the _____ Division of the _____ Court Department.

Date Issued	Signature of Justice, Clerk-Magistrate or Assistant Clerk X _____
First or Administrative Justice **WITNESS:** _____	Printed name of Justice, Clerk-Magistrate or Assistant Clerk

1296

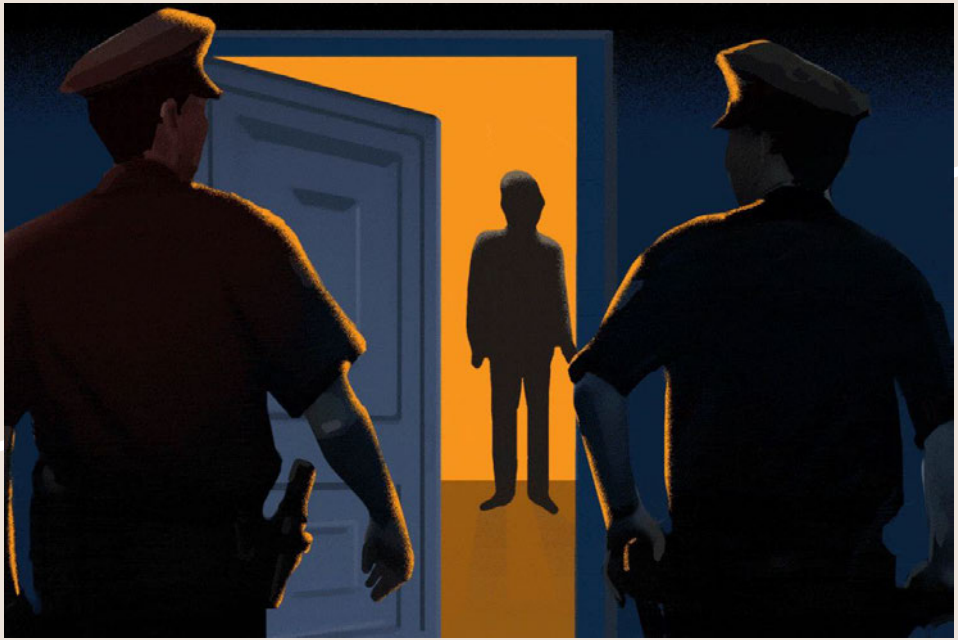
The Warrant

IMPORTANT - Make sure to attach the Addenda to the warrant. Failure to do so will result in suppression!



- ➔ Permissions - If your affidavit sets forth probable cause for a nighttime search, no knock warrant, or to search persons on the premises, be sure to check the appropriate boxes!
- ➔ District Court with jurisdiction over the crime - the Court to which the warrant will be returned.
- ➔ Signatures - Make sure the judge or clerk signs and dates the warrant in addition to the affidavit.
- ➔ Witness - For Superior Court warrant, print name of the Adminstrative Justice (currently Justice Heidi J. Brieger). For District Court, insert Presiding Justice of applicable District Court division.

Search Warrant Execution



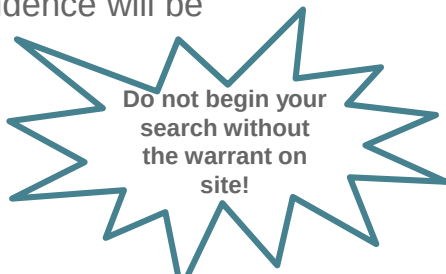
Securing the Premises

Secure from Outside if:

- ➔ **Legitimate concerns evidence will be destroyed or removed** - secure perimeter of premises for a reasonable time while obtaining the Search Warrant;
- ➔ **No objectively reasonable belief the premises are occupied**; or
- ➔ **Occupants have left the premises**

Secure from Within ONLY IF:

- ➔ There is specific information (amounting to probable cause) supporting an objectively reasonable belief that evidence will be destroyed or removed.



Before You Execute the Warrant . . .



- The Search Warrant must be **on the premises** before the search may begin.
- Show the Search Warrant to the person in control of the premises (if possible), and a copy may be left at the scene.
- Double check that **ALL ADDENDA ARE ATTACHED TO THE SEARCH WARRANT.**

Entering the Premises

Requirements: Knock and announce presence and purpose

1300

How Long to Wait After Knocking:

- ➔ Depends on circumstances. E.g., if you have knowledge of presence of weapons in small apartment, 5 seconds is sufficient

You May Use Forcible Entry ONLY IF:

- ➔ Occupant refuses to admit you;
- ➔ No response after waiting reasonable time;

Use of Ruse

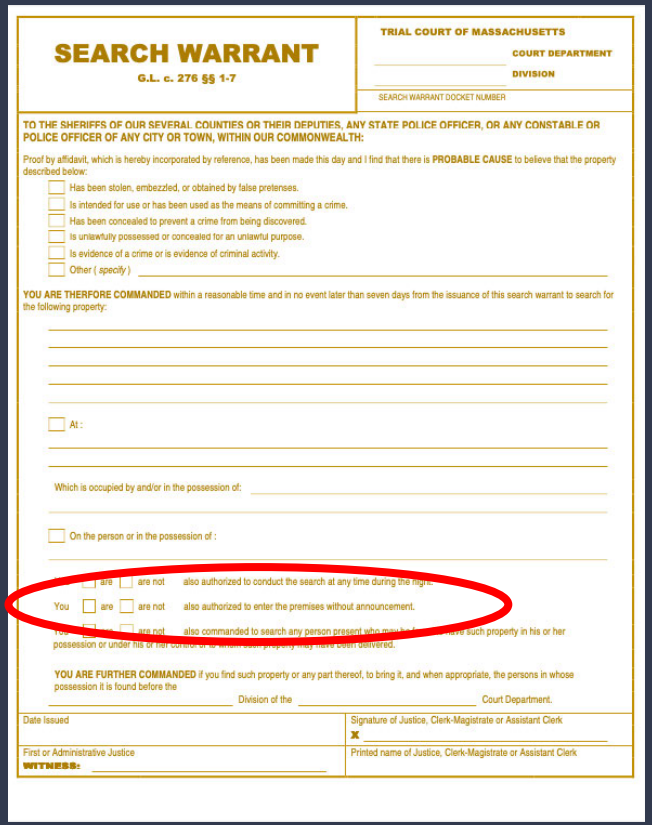
- ➔ OK if used to decrease potential for violence

Detaining Occupants

- ➔ May detain during search but not while waiting for search warrant

1301

“No Knock” Entry



SEARCH WARRANT
G.L. c. 276 §§ 1-7

TRIAL COURT OF MASSACHUSETTS
COURT DEPARTMENT
DIVISION
SEARCH WARRANT DOCKET NUMBER

TO THE SHERIFFS OF OUR SEVERAL COUNTIES OR THEIR DEPUTIES, ANY STATE POLICE OFFICER, OR ANY CONSTABLE OR POLICE OFFICER OF ANY CITY OR TOWN, WITHIN OUR COMMONWEALTH:

Proof by affidavit, which is hereby incorporated by reference, has been made this day and I find that there is **PROBABLE CAUSE** to believe that the property described below:

- ☐ Has been stolen, embezzled, or obtained by false pretenses.
- ☐ Is intended for use or has been used as the means of committing a crime.
- ☐ Has been concealed to prevent a crime from being discovered.
- ☐ Is unlawfully possessed or concealed for an unlawful purpose.
- ☐ Is evidence of a crime or is evidence of criminal activity.
- ☐ Other (*specify*) _____

YOU ARE THERFORE COMMANDED within a reasonable time and in no event later than seven days from the issuance of this search warrant to search for the following property:

☐ At :

Which is occupied by and/or in the possession of: _____

☐ On the person or in the possession of :

You ☐ are ☐ are not also authorized to conduct the search at any time during the night.

You ☐ are ☐ are not also authorized to enter the premises without announcement.

You ☐ are ☐ are not also commanded to search any person present who may have such property in his or her possession or under his or her control or in which such property may have been delivered.

YOU ARE FURTHER COMMANDED if you find such property or any part thereof, to bring it, and when appropriate, the persons in whose possession it is found before the _____ Division of the _____ Court Department.

Date Issued	Signature of Justice, Clerk-Magistrate or Assistant Clerk X _____
First or Administrative Justice **WITNESS:** _____	Printed name of Justice, Clerk-Magistrate or Assistant Clerk

Permission for no knock MUST be requested on the Search warrant

- Mass. General Laws c.276 § 2D
  - Search Warrant affidavit must establish probable cause that if the law enforcement officer announces their presence their life or the lives of others will be endangered

AND

  - Include an attestation that the law enforcement officer filing the affidavit has no reason to believe that minor children or adults over the age of 65 are in the home, unless there is a credible risk of imminent harm to the minor or adult over the age of 65 in the home.

- Must conduct threshold reappraisal of probable cause at time of warrant execution.

1302

Documenting the Search



- Appoint one officer to be the “evidence officer” to:
    - take custody of evidence as it is found;
    - note type of evidence and location where found; and
    - photograph or facilitate photography of evidence before moving it from the place in which it was discovered.
- Video and Photography
    - Authority to videotape or photograph the search is limited to:
        - documenting evidence authorized to be seized by the warrant (or discovered in plain view) in order to preserve its condition and location and
        - Recording the condition of the search scene to protect police from allegations of damage.

Scope of the Search: Curtilage and Cars

An area is within the curtilage of a residence only when it is “so intimately tied to the home itself” that “an individual reasonably may expect that the area in question [will] be treated as the home itself.”

To assess whether an area is within the home’s curtilage, look at:

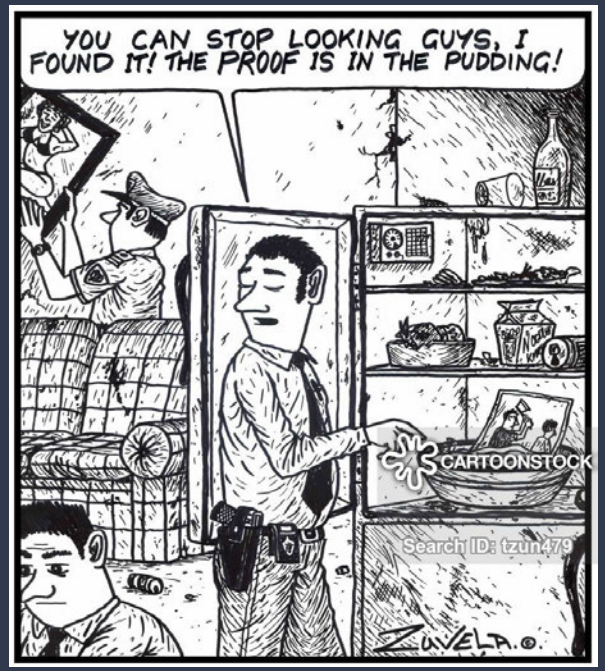
- ➔ The proximity of the area to the home;
- ➔ Whether the area is included within an enclosure surrounding the home;
- ➔ The use of the area; and
- ➔ Steps taken by resident to protect area from observations by passers-by

Automobiles: If an automobile is controlled by the owner of the residence and located within the curtilage, it may be searched.

TIP: When in doubt, include cars, outbuildings, and common areas to which the target has access in the warrant!

1304

Scope of the Search: Containers

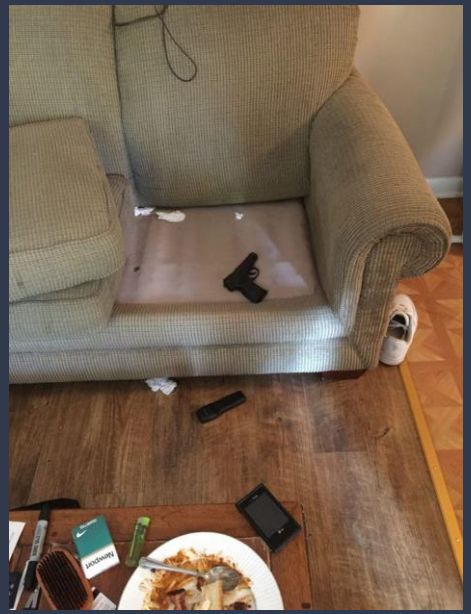


- ➔ Locked or unlocked containers on the premises that reasonably could contain or conceal an item described in the search warrant may be opened and searched.

- ➔ If necessary, police may damage or destroy property in order to execute a search warrant.

1305

Plain View Observations



In order to seize contraband NOT listed in the warrant:

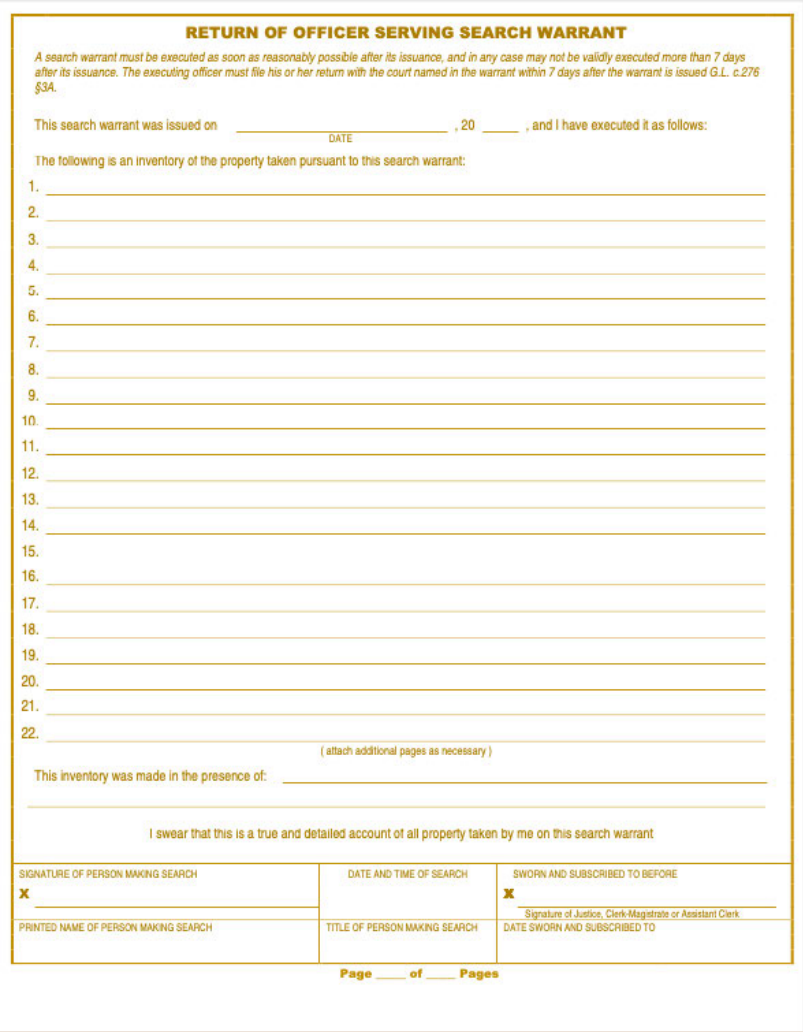
- ➔ It must be readily apparent that the item is incriminating;
- ➔ The evidence must be observed from a location that police have a right to be; and
- ➔ The discovery of the item must be inadvertent.

TIP: If the contraband in plain view creates probable cause to believe there will be other related contraband in the area, **freeze the scene and apply for another warrant.**

Search Warrant Return

Return should be:

- Made to District Court with territorial jurisdiction over crime (required) and
- Made by officer present during execution of warrant (recommended).



RETURN OF OFFICER SERVING SEARCH WARRANT

A search warrant must be executed as soon as reasonably possible after its issuance, and in any case may not be validly executed more than 7 days after its issuance. The executing officer must file his or her return with the court named in the warrant within 7 days after the warrant is issued G.L. c.276 §3A.

This search warrant was issued on _____ (DATE), 20 ____, and I have executed it as follows:

The following is an inventory of the property taken pursuant to this search warrant:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____
11. _____
12. _____
13. _____
14. _____
15.
16. _____
17. _____
18. _____
19. _____
20. _____
21. _____
22. _____

(attach additional pages as necessary)

This inventory was made in the presence of: _____

I swear that this is a true and detailed account of all property taken by me on this search warrant

SIGNATURE OF PERSON MAKING SEARCH	DATE AND TIME OF SEARCH	SWORN AND SUBSCRIBED TO BEFORE
X _____		X _____ Signature of Justice, Clerk-Magistrate or Assistant Clerk
PRINTED NAME OF PERSON MAKING SEARCH	TITLE OF PERSON MAKING SEARCH	DATE SWORN AND SUBSCRIBED TO

Page ____ of ____ Pages

1307

Time Limitations



July 2020

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
			1	Apply	1.	2.
3.	4.	5.	6.	Return	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

- ➔ The Search warrant must be executed AND returned as soon as reasonably possible, but in no event later than 7 days after issuance

- ➔ REMEMBER:
  - The day on which the warrant issued is not included in the computation and
  - Saturdays, Sundays, and legal holidays are included

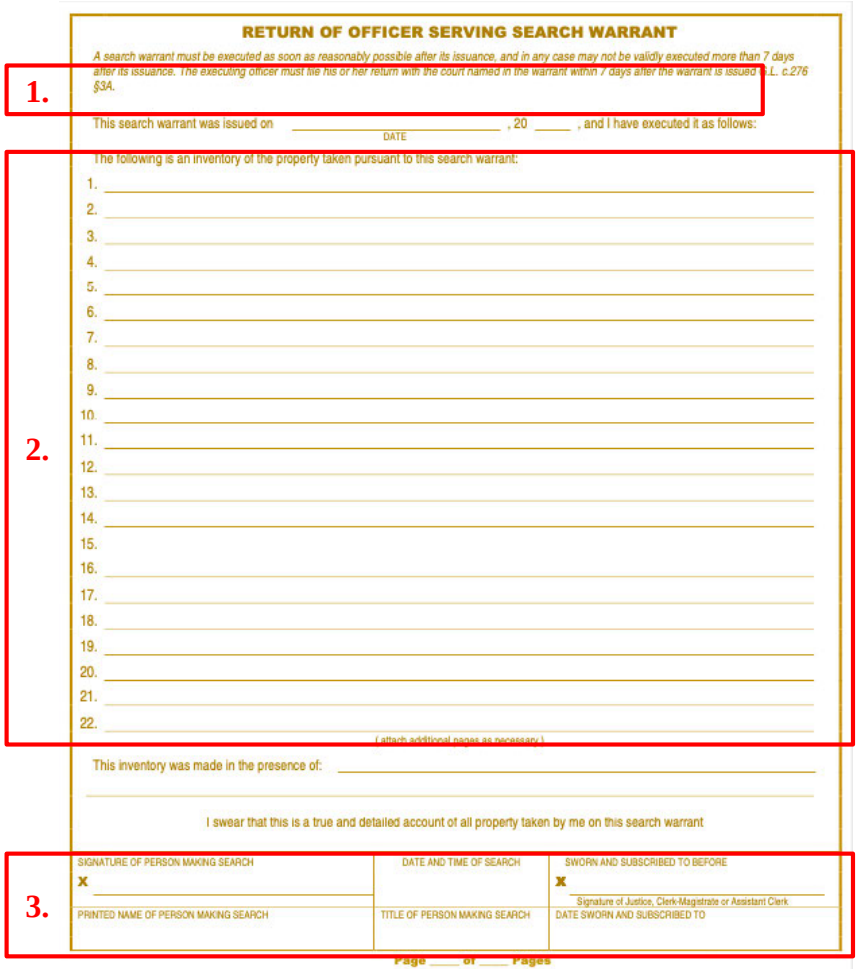
Search Warrant Return

- ➔ Remember - the search warrant must be returned within 7 days even if still waiting for response from service provider OR completion of forensic exam!
- ➔ List ALL property seized!
  - When waiting for a response from service provider or forensic exam, include:

"A search warrant for [DEVICES] was executed on [DATE]. The [cell phones and/or computers] have been delivered to [NAME] for analysis. Such analysis will take longer than seven days to complete. Any information received pursuant to the terms of the warrant will be turned over in the course of discovery in accordance with the Commonwealth's obligations."

- ➔ Have clerk attest to your signature upon return

TO BE COMPLETED BY OFFICER WHO EXECUTED WARRANT



RETURN OF OFFICER SERVING SEARCH WARRANT

A search warrant must be executed as soon as reasonably possible after its issuance, and in any case may not be validly executed more than 7 days after its issuance. The executing officer must file his or her return with the court named in the warrant within 7 days after the warrant is issued. G.L. c.276 §3A.

1.

This search warrant was issued on _____ (DATE), 20 ____, and I have executed it as follows:

2.

The following is an inventory of the property taken pursuant to this search warrant:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____
11. _____
12. _____
13. _____
14. _____
15. _____
16. _____
17. _____
18. _____
19. _____
20. _____
21. _____
22. _____

(attach additional pages as necessary)

This inventory was made in the presence of: _____

I swear that this is a true and detailed account of all property taken by me on this search warrant

3.

SIGNATURE OF PERSON MAKING SEARCH	DATE AND TIME OF SEARCH	SWORN AND SUBSCRIBED TO BEFORE
X _____		X _____ Signature of Justice, Clerk-Magistrate or Assistant Clerk
PRINTED NAME OF PERSON MAKING SEARCH	TITLE OF PERSON MAKING SEARCH	DATE SWORN AND SUBSCRIBED TO

Page ____ of ____ Pages

1309

Impoundment



Once the search warrant is returned, it becomes a public document unless we file a motion to impound!

- ➔ When is impoundment appropriate?
  - Preserving secrecy of ongoing investigation;
  - Protecting against potential dangers of pretrial publicity; and/or
  - Guarding privacy interests of victim or victim's family.

- ➔ How to impound the warrant:
  - Speak to the assigned ADA to determine if there are legal grounds to impound the warrant;
  - The ADA will draft a motion to impound to be presented to the judge either at the time of application or at the time of return.

TIP: When an affidavit seeks evidence in a sexual assault investigation, use the victim's name only ONCE and then refer to "victim" throughout the affidavit.

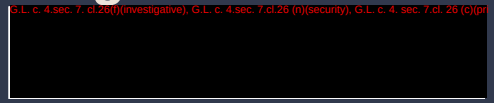
1310

SEARCH WARRANT TEAM

ADA Jamie Charles, Captain
ADA Tim Ferriter, Deputy Captain

➔ ***Office Hours***
(781) 897-6825

➔ ***Nights and Weekends (emergency matters)***



700 CMR 7.00: USE OF THE MASSACHUSETTS TURNPIKE AND THE METROPOLITAN HIGHWAY SYSTEM

Section

7.01: Scope and Effect
7.02: Definitions
7.03: Tolls
7.04: EZDriveMA Toll Collection
7.05: EZDriveMA Toll Enforcement
7.06: Limitations on Use of Ways
7.07: Special Limitations and Issuance of Special Permits
7.08: Limitations on Large Tandem Units
7.09: Traffic, Operation, and Safety
7.10: Motor Carrier Safety Act
7.11: Hazardous Materials
7.12: Repair or Removal of Vehicle
7.13: Penalties
7.14: Parking Violation Enforcement

7.01: Scope and Effect

(1) Scope. 700 CMR 7.00 regulates activity, and establishes procedures, requirements, and penalties, with respect to the use of ways under the jurisdiction of the Massachusetts Department of Transportation. A provision of 700 CMR 7.00 applies equally to each such way, whether or not the provision refers explicitly to a way, unless the provision states otherwise.

(2) Effect. The headings of 700 CMR 7.00 are provided for ease of reference only and should not be used to construe its provisions. A judicial determination that a provision of 700 CMR 7.00 is unenforceable does not affect another provision of 700 CMR 7.00 unless the provisions are integrally related and cannot be severed.

7.02: Definitions

The following terms and their grammatical counterparts are used in 700 CMR 7.00 as described in 700 CMR 7.02:

Abandoned Vehicle refers to a vehicle other than a disabled vehicle left on a way with neither the operator nor another responsible individual present.

Acceleration Lane refers to a special travel lane on a way that facilitates a change of speed by a vehicle entering a travel lane.

Account Holder is an E-ZPass MA or Pay By Plate customer who uses the EZDriveMA system in accordance with applicable rules, regulations and/or terms and conditions.

ALPR shall mean Automatic License Plate Recognition which are automated computer processes that identify a license plate number, state from which the license plate was issued, and/or license plate type using optical character recognition or similar software.

Apportioned Vehicle refers to a motor vehicle bearing a valid number plate with an "apportioned" designation issued by the Massachusetts Registrar of Motor Vehicles or an equivalent number plate.

Articulated Bus refers to the term "articulated bus" as defined in M.G.L. c. 90, § 1.

Auto Home refers to the term "auto home" as defined in M.G.L. c. 90, § 1.

Automobile Transporter refers to the term "automobile transporter" as defined in M.G.L. c. 90, § 1. A tractor-trailer or semi-trailer unit capable of transporting fully-assembled automobiles or other types of cargo within the enclosed trailer in a tractor-trailer unit or within the enclosed semi-trailer in a semi-trailer unit is not an "automobile transporter" for the purposes of 700 CMR 7.02.

7.02: continued

Axle refers to a supporting structure, upon which a pair or pairs of wheels revolve, that may be included between two parallel transverse vertical planes forty inches apart extending across the full width of the supported vehicle.

Balance Due the amount shown on invoices and/or other notices, which includes the amount due for tolls, fines, and other fees owed to MassDOT for use of the Massachusetts Turnpike, MHS, or MassDOT owned or MassDOT approved facilities.

Boat Transporter refers to the term "boat transporter" as defined in M.G.L. c. 90, § 1.

Boston Extension refers to the roadways and tunnels for vehicular traffic as defined in M.G.L. c. 6C, § 1.

Boston Extension Tunnel refers to the vehicular tunnel consisting of two roadways separated by a median under the air rights project between Dalton Street and Clarendon Street, including Interchange 22, in the city of Boston, and any additional area that the Department designates as such.

Breakdown Lane refers to a paved lane on a way to the right of the travel lanes and separated from them by a solid line.

Bridge Gross Weight Formula refers to the formula and definitions of terms set out in 700 CMR 7.07(3)(b).

Bus refers to a motor vehicle bearing a valid number plate with a "bus" designation issued by the Massachusetts Registrar of Motor Vehicles or an equivalent number plate.

Callahan Tunnel refers to the tunnel for vehicular traffic as described and defined in M.G.L. c. 6C, § 1.

Car Pool Vehicle refers to a private passenger motor vehicle, not for public hire, carrying three or more occupants, one of whom possesses a currently valid car pool identification card.

Chief Engineer refers to the Chief Engineer of the Department or an employee or employees of the Department designated by the Chief Engineer to carry out one or more of the responsibilities assigned to the Chief Engineer in accordance with 700 CMR 7.00.

Clerk shall mean MassDOT employees, hearing examiners, or persons employed by or under contract with MassDOT or its EZDriveMA system contractor, designated by MassDOT to review and to perform functions related to EZDriveMA such as processing transactions, invoicing, disputes, appeals and hearings, and to administer and/or enforce collections or other liabilities and tasks associated with the EZDriveMA system.

Commercial Vehicle shall mean any Motor Vehicle which is not a Private Passenger Motor Vehicle displaying a private passenger registration number plate issued by the Massachusetts Registrar of Motor Vehicles or other jurisdictions or an equivalent number plate and is not a Motorcycle displaying a Motorcycle registration number issued by the Massachusetts Registrar of Motor Vehicles or other jurisdictions or an equivalent number plate.

Creeper Lane refers to a special travel lane on a way provided for vehicles that cannot maintain the required rate of speed over travel lanes.

Cross-over refers to an area in a median used by a vehicle authorized in accordance with 700 CMR 7.09(10)(b) to cross a median.

Deceleration Lane refers to a special travel lane on a way that facilitates a change of speed by a vehicle leaving a travel lane.

Department or MassDOT refers to the Massachusetts Department of Transportation created by M.G.L. c. 6C.

7.02: continued

Department Vehicle refers to a vehicle owned by the Department and operated by one of its employees or a Massachusetts Troop E State Police officer.

Disabled Vehicle refers to a vehicle on a way that is incapable of movement under its own power or as to which movement is inadvisable because of a flat tire, mechanical breakdown, or other malfunction. A disabled vehicle is not an abandoned vehicle provided that it is not stopped on a way for a period of more than two hours and that the Massachusetts State Police have been notified that the vehicle is disabled.

Equivalent Number Plate refers to a type of number plate issued by the Registrar or department of motor vehicles or similar official or department of another jurisdiction in accordance with the law of that jurisdiction that is equivalent in function and designation to the specific type of number plate issued by the Massachusetts Registrar of Motor Vehicles that 700 CMR 7.00 requires a vehicle registered in Massachusetts to display.

EZDriveMA is the cashless, automated system installed on or operating with respect to the Massachusetts Turnpike, MHS, a way, or at other MassDOT owned or MassDOT approved facilities for the purpose of collecting tolls, fares, fees, fines or other transactions as determined by MassDOT. The EZDriveMA system consists of E-ZPass MA and Pay By Plate.

E-ZPass MA Equipped Motor Vehicle shall mean a motor vehicle properly equipped with and using a valid electronic device, such as a transponder, that MassDOT, or its E-ZDrive MA system contractor has issued or authorized for the purpose of transmitting information to the EZDriveMA system for collecting tolls, fares, fines, fees or other transactions electronically

E-ZPass MA shall mean the electronic toll collection system installed on or operating with respect to the Massachusetts Turnpike, a way, or at other MassDOT owned or MassDOT approved facilities for the purpose of collecting tolls, fares, fines, fees or other transactions through an electronic device, such as a transponder, as determined by MassDOT.

Explosive refers to any chemical compound, mixture, or device, the primary or common purpose of which is to function by explosion, *i.e.*, with substantially instantaneous release of gas and heat.

Fullmount refers to a smaller vehicle mounted completely on the frame of either the first or last vehicle in a saddlemount combination.

Gross Vehicle Weight Rating refers to the term "gross vehicle weight rating" as defined in M.G.L. c. 90, § 1.

Hazardous Material refers to the term "hazardous material" as defined in 49 CFR Parts 171 through 173 and 177.

Hearse refers to a motor vehicle bearing a valid number plate with a "hearse" designation issued by the Massachusetts Registrar of Motor Vehicles or an equivalent number plate.

Heavy Commercial Vehicle refers to a vehicle in excess of 2.5 tons that is used for the transportation of goods, wares, or merchandise.

High Occupancy Vehicle refers to a bus, a car pool vehicle, a pupil vehicle, a school bus, or a vanpool vehicle.

Hot List - a list of specific license plates and/or transponder numbers provided or identified by law enforcement to MassDOT pursuant to the standards and procedures in 700 CMR 7.05(8).

House Trailer refers to the term "house trailer" as defined in M.G.L. c. 90, § 1.

Interchange refers to a location that provides entry to and/or exit from a way.

7.02: continued

Irreducible Load or Vehicle refers to a load or vehicle exceeding applicable weight or length limitations under 700 CMR 7.07 that, if separated into smaller loads or vehicles, would compromise the intended use of the vehicle, *i.e.*, make it unable to perform the function for which it was intended; destroy the value of the load or vehicle, *i.e.*, make it unusable for its intended purpose; or require more than eight work hours to dismantle using appropriate equipment.

Irreducible Load Permit refers to a permit that the Department issues for use of a way in accordance with 700 CMR 7.07(3)(c)1. or (4)(c)1.

Lane refers to a longitudinal strip of roadway of sufficient width to accommodate the passage of a single line of vehicles, whether or not the bounds of the lane are indicated by pavement markings or longitudinal construction joints.

Large Tandem Unit refers to a tandem unit in which either the semi-trailer or trailer exceeds 28 feet in length.

Large Tandem Unit Permit refers to a permit that the Department issues in accordance with 700 CMR 7.08.

Late Fee is assessed by MassDOT on unpaid tolls and/or other transactions that have not been paid in full by the Payment Due Date shown on an invoice or notice.

Livery Vehicle refers to a motor vehicle bearing a valid number plate with a "livery" designation issued by the Massachusetts Registrar of Motor Vehicles or an equivalent number plate.

Marking refers to a line, legend, or other medium or device that is painted or placed by or at the direction of the Department on the surface of a way.

Massachusetts State Police Officer refers to a state police officer assigned to the Department under the provisions of M.G.L. c. 22C, § 29.

MassDOT or Department refers to the Massachusetts Department of Transportation created by M.G.L. c. 6C.

Median refers to the area separating traffic moving in opposite directions on a way.

Metropolitan Highway System (MHS) refers to the highway system that consists of the Boston Extension, the Callahan Tunnel, the Central Artery, the Central Artery North Area, the Sumner Tunnel, and the Ted Williams Tunnel, as defined in M.G.L. c. 6C, § 1.

Motorcycle refers to the term "motorcycle" as defined in M.G.L. c. 90, § 1.

Motor Vehicle refers to the singular of the term "motor vehicle" as defined in M.G.L. c. 90, § 1.

Non-revenue Vehicle refers to an official vehicle of the Department and any other vehicle that the Department designates as such.

Official Emergency Vehicle refers to an official police, fire, or health services vehicle of Massachusetts or any of its municipalities, political subdivisions, or instrumentalities.

Official Vehicle of the Department refers to a motor vehicle of a member, officer, or employee of the Department or of a person engaged in the performance of duties in connection with the operation of a way.

On The Go (OTG) is a prepaid toll payment option through use of a transponder or other electronic device issued by MassDOT or its EZDriveMA contractor, for use with the EZDriveMA system, and said device has not been registered with MassDOT or other agency or entity that has toll collection reciprocity with MassDOT.

7.02: continued

Operator refers to an individual who operates a motor vehicle.

Over-size Vehicle refers to a vehicle or vehicle combination that exceeds the maximum size designated for a vehicle or vehicle combination of its type as specified in 700 CMR 7.07(4)(a).

Over-weight Vehicle refers to a vehicle that exceeds the maximum weight designated for a vehicle of its type as specified in 700 CMR 7.07(3) and/or 7.08(4).

Parked Vehicle refers to a vehicle that is stopped or standing, whether occupied or not, except that a vehicle is not a parked vehicle if it has stopped temporarily because its movement is obstructed, the operator is following the direction of a Massachusetts State Police officer or a sign, or because it is a disabled vehicle.

Parking refers to the stopping or standing of a parked vehicle.

Pay By Plate (PBP) refers to the EZDriveMA payment option where photographic or video images of vehicles and license plates are used to either post toll transactions to a Registered Pay By Plate account or for obtaining the name and address of the registered owner of the vehicle from the Registry of Motor Vehicles/Department of Motor Vehicles (RMV/DMV) or other means, for purposes of collecting tolls, fees, fines, and other debts owed.

Pay By Plate Invoice refers to an itemized statement issued to a vehicle's registered owner of record or responsible party, where applicable, which provides a summary of toll usage, tolls due, balance, late and other fees, fines, penalties, and other amounts due associated with toll or other transactions, as well as payments made, and/or credits.

Pay By Plate Notice of Non-payment (NONP) is a statement issued to a vehicle's registered owner of record, or other responsible party, where applicable, when any portion of the Balance Due from the Pay By Plate Past Due Invoice is outstanding after the Pay By Plate Past Due Invoice Payment Due Date. The NONP may include any previous Balance Due and any current tolls, fees, fines, penalties and other amounts due, as well as payments made, credits, and/or other transactions.

Pay By Plate Notice of Liability (NOL) is a statement issued to a vehicle's registered owner of record when any portion of the Balance Due from the NONP is outstanding after the NONP Payment Due Date. The NOL may include any previous Balance Due and any current tolls, fees, fines and penalties, as well as payments made credits, and/or other transactions. The NOL demands immediate payment of NOL Balance Due.

Pay By Plate Past Due Invoice refers to a statement issued to a vehicle's registered owner or other responsible party, where applicable, when any portion of the Balance Due from the Pay By Plate Invoice is outstanding after the Pay By Plate Invoice Payment Due Date. Pay By Plate Past Due Invoice may include any previous Balance Due and any current tolls, fees, fines, penalties, and other amounts due, as well as payments made, credits, and/or other transactions.

Pay By Plate Registered Account refers to a payment option whereby a vehicle and its corresponding license plate is provided by the customer to be listed on an account for collecting tolls, fees, fines or other transactions as determined by MassDOT.

Payment Due Date is the date on which a payment must be received by MassDOT in accordance with an E-ZPass MA or Pay By Plate invoice or notice issued by MassDOT in order to avoid additional fees, fines, and/or penalties.

Person refers to an individual, firm, co-partnership, association, corporation, or other legal entity.

Private Passenger Motor Vehicle refers to the term "private passenger motor vehicle" as defined by the Registrar of Motor Vehicles in 540 CMR 2.05: *Vehicle Registration Requirements.*

Pupil Vehicle refers to a motor vehicle bearing a valid number plate with a "pupil" designation issued by the Massachusetts Registrar of Motor Vehicles or an equivalent number plate.

7.02: continued

Qualified Towing Contractor refers to a qualified emergency road-service provider having a service contract with the Department in accordance with 700 CMR 7.12(2)(c)3.

Recreational Vehicle refers to a private passenger motor vehicle that provides living accommodations for persons or an apportionable vehicle designed or converted and used exclusively for personal pleasure or travel by an individual or the individual's family.

Reducible Load refers to any load or object including the vehicle whose gross weight or dimensions can be practically reduced to a lesser gross weight or dimension as determined by the Chief Engineer.

Reducible Load Permit refers to a permit that the Department issues to an owner or lessee of a vehicle for which the chief engineer has issued a valid reducible load permit in accordance with 700 CMR 7.07(3)(c)3.

Registered Owner refers to a person registered by the Massachusetts Registrar of Motor Vehicles in accordance with M.G.L. c. 90, § 2, at the time of a violation of 700 CMR 7.03, 7.04, or 7.12 as the owner of the vehicle involved in the violation or who is so registered by the Registrar or department of motor vehicles or similar official or department of another jurisdiction in accordance with the law of that jurisdiction.

Roadway refers to that portion of a way consisting of travel lanes, including acceleration lanes and deceleration lanes, creeper lanes, and ramps or approaches to toll plazas.

Saddlemount Combination refers to a combination of vehicles in which a truck or tractor tows one or more trucks or tractors, each connected by a saddle to the frame or fifth wheel of the vehicle in front of it. The saddle is a mechanism that connects the front axle of the towed vehicle to the frame or fifth wheel of the vehicle in front of the towed vehicle and functions as a fifth wheel kingpin connection. When two vehicles are towed in this manner, the combination is called a double saddlemount combination, and, when three vehicles are towed in this manner, the combination is called a triple saddlemount combination.

School Bus refers to a motor vehicle bearing a valid number plate with a "school bus" designation issued by the Massachusetts Registrar of Motor Vehicles or an equivalent number.

Semi-trailer refers to the term "semi-trailer" as defined in M.G.L. c. 90, § 1. Semi-trailer unit refers to the term "semi-trailer unit" as defined in M.G.L. c. 90, § 1.

Service or Rest Area refers to an area that the Department designates along a way for the purpose of providing travelers on the way rest or refreshment or to provide services for vehicles using the way.

Shoulder refers to that part of the paved surface of a way lying outside solid traffic lines.

Sign refers to a sign, lights, signal, barrier, marker, marking, cone, barrel, or similar device or indicator, whether the means of display or indication is mechanical, electrical, acoustical, or another means, that the Department deploys or causes to be deployed for the purpose of regulating traffic, parking, or other activity on a way.

Small Tandem Unit refers to a tandem unit in which either the semi-trailer or trailer does not exceed 28 feet in length.

Small Tandem Unit Permit refers to a permit that the Department issues in accordance with 700 CMR 7.07(3)(c)(4).

Special Fuel refers to a liquefied petroleum gas, including propane, butane, LP Gas or LPG, a liquefied natural gas or LNG, and a compressed natural gas or CNG.

7.02: continued

Special Fuel Transportation Permit refers to a permit that the Department issues allowing a vehicle transporting a special fuel to travel on certain portions of a way in accordance with 700 CMR 7.07(6).

Special Permit refers to an irreducible load permit, a large tandem unit permit, a small tandem unit permit, a reducible load permit, a special permit for explosives, or a special fuel transportation permit.

Special Permit for Explosives refers to a permit that the Department issues allowing a vehicle transporting explosives to travel on certain portions of a way in accordance with 700 CMR 7.07(5).

Special Vehicle refers to a vehicle that is not otherwise a commercial vehicle or high-occupancy vehicle and that the Department designates as authorized to use the Tunnels in furtherance of a purpose or need consistent with the public welfare or necessity and with the safe and efficient use of the Tunnels.

Sumner Tunnel refers to the tunnel for vehicular traffic as defined in M.G.L. c. 6C, § 1.

Tandem Axles refers to two or more consecutive axles whose centers can be included between parallel transverse vertical planes spaced not less than 40 and not more than 96 inches apart, extending across the full width of the vehicle.

Tandem Unit refers to the term "tandem unit" as defined in M.G.L. c. 90, § 1.

Taxi refers to a motor vehicle bearing a valid number plate with a "taxi" designation issued by the Massachusetts Registrar of Motor Vehicles or an equivalent number plate.

Ted Williams Tunnel refers to the system of roadways, bridges, viaducts and tunnels for vehicular traffic as defined in M.G.L. c. 6C, § 1.

Toll shall mean the amount assessed by MassDOT for passage over the Massachusetts Turnpike and MHS.

Tractor refers to the non-cargo carrying power unit that operates in combination with a semi-trailer or trailer, except that the power unit of a semi-trailer unit engaged in the transportation of automobiles is also a tractor notwithstanding its use to carry motor vehicles.

Traffic refers to vehicles, either singly or together, using any portion of a way for the purpose of travel.

Traffic Control Signal refers to a device using colored lights whereby traffic may alternately be directed to slow down and proceed with caution, to stop, or to proceed.

Trailer refers to the term "trailer" as defined in M.G.L. c. 90, § 1.

Transponder refers to an electronic device used for the collection of tolls, fines, or other fees as determined by MassDOT.

Travel Lane refers to a lane used by traffic for ordinary travel.

Truck refers to a motor vehicle designed to carry goods.

Tunnels refers to all Tunnels owned and operated by the Department, Metropolitan Highway System Tunnels, including but not limited to the Callahan, Sumner, Ted Williams, Boston Extension as defined in M.G.L. c. 6C, § 1, including the roadway referred to as the Prudential Tunnel, I-90, I-93, and the Central Artery North Area (CANA) Tunnels, individually or collectively, including their access and egress ramps, each of which is a way.

7.02: continued

Turnpike refers to the term "turnpike" as defined in M.G.L. c. 6C, § 1.

U-turn refers to the backing or turning of a vehicle whereby its direction is reversed.

Vanpool Vehicle refers to a motor vehicle bearing a valid number plate with a "vanpool" designation issued by the Massachusetts Registrar of Motor Vehicles or an equivalent number plate.

Vehicle refers to a device in, upon, or by which individuals or property are or can be transported upon a way.

Vehicle Combination refers to any attached combination of a motor vehicle and vehicle or vehicles.

Vehicle Height refers to the height of a vehicle, including its load.

Vehicle Length refers to the length of a vehicle or vehicle combination, including its load and load-holding devices, but exclusive of safety and energy-conservation devices such as refrigeration units and air compressors, heating units, wind deflectors, flexible fender extensions, mud flaps and splash and spray suppressant devices, or other device that the Department determines is necessary for safe and efficient operation, provided that any such device is mounted, and extends beyond the nominally allowed length, in a manner and to the extent that the Department determines, and provided further that the device is not designed or used to carry cargo.

Vehicle Weight refers to the gross weight of a vehicle, including its load.

Vehicle Width refers to the width of a vehicle, including its load, but exclusive of load-induced tire bulge, rear view mirrors, turn signal lamps, hand holds for cab entry or egress, mud flaps and splash and spray suppressant devices, or other device that the Department determines is necessary for the safe and efficient operation of the vehicle, provided that any such device is mounted, and extends beyond the nominally allowed width, in such manner and to such extent as the Department determines, and provided further that in no event may such a device extend more than three inches beyond the maximum vehicle width on each side.

Way is defined as the Turnpike, the Metropolitan Highway System, tunnels, a service or rest area, that is located on property owned or controlled and under the jurisdiction of the Department, and includes the areas appurtenant to said way that are necessary for the operation, construction and maintenance of the way.

7.03: Tolls

(1) Vehicle Classification. The Department applies the vehicle classification schedules specified in 700 CMR 7.03(1): *Table 1*, to determine tolls for the use of a way for which the Department collects a toll. (*See* Note 1).

TABLE 1

Class	Type of Vehicle
2	Private Passenger 2 Axles
2	Resident Program Commuter ** 2 Axles
2	Commercial - 2 Axle
3	Any 3 Axle Vehicle
4	Any 4 Axle Vehicle
5	Any 5 Axle Vehicle

7.03: continued

Class	Type of Vehicle
6	Any 6 Axle Vehicle
7	Any 7 Axle Vehicle
8	Any 8 Axle Vehicle
9	Any 9 Axle Vehicle
10	Any 10 Axle Vehicle
11	Any 11 Axle Vehicle
12	Any 12 Axle Vehicle
13	Any 13 Axle Vehicle
14	Any 14 Axle Vehicle
15	Any 15 Axle Vehicle

* Motor Vehicle Description determined by type of registration (Massachusetts vehicles) or by image and/or type of vehicle (non Massachusetts vehicles).

Note 1. Toll Rates may vary for vehicles qualifying for specific toll rate Programs established by the Department.

(2) Payment of Toll. Each Operator shall pay the toll as established by MassDOT. MassDOT may obtain an image of the vehicle and/or vehicle license plate for purposes of assessing a toll, invoicing, assessing fees, fines, and/or penalties; evaluating transaction disputes and appeals; and toll collection and violation enforcement.

(3) Evasion of Toll. No person may commit, or attempt to commit, any act with the intent to evade the payment of a toll or to defraud the Department with respect to the payment of a toll. Refusal to pay a toll are both considered to be acts done with intent to evade the payment of a toll.

(4) Special Permit Fees. The operator of a motor vehicle requiring a special permit for use of a way shall pay the fee that the Department determines in accordance with the provisions of the permit and of 700 CMR 7.07.

(5) Car Pool Program. Only authorized E-ZPass MA equipped vehicles will be eligible for the car pool program. Qualifying individuals who choose to participate in the car pool program shall adhere to the E-ZPass MA terms and conditions and regulations governing the use of the EZDriveMA system and the car pool program. To be eligible for the car pool program, qualifying individuals shall renew on an annual basis. Qualifying individuals must submit on an annual basis a valid Massachusetts Registry of Motor Vehicles registration and/or lease agreement, and a valid driver's license. Failure to renew by the applicable expiration date will result in the loss of the car pool program discount. While not in the program, the subject individual shall be responsible for the full toll rate and the full, non discounted toll rate.

(6) Vehicle Classification. Each motor vehicle displaying a private passenger registration number plate or a motorcycle displaying a motorcycle registration number plate shall pay the toll established by MassDOT for a Private Passenger Motor Vehicle, provided such vehicles are listed on a Private Passenger Account. Each motor vehicle which does not display a private passenger registration number plate or a motorcycle registration number plate, or any private passenger registration or motorcycle that is listed on a Commercial Account shall pay the toll established by MassDOT for a Commercial Motor Vehicle. Toll rates may vary depending upon the method in which the toll was assessed.

7.03: continued

(7) Resident Discount Program. Only authorized E-ZPass MA equipped vehicles will be eligible for the resident discount program. Residents who qualify and choose to participate in the resident discount program shall adhere to the E-ZPass MA terms and conditions and regulations governing the use of the EZDriveMA system. To be eligible for the resident discount program, qualifying Boston residents shall renew on an annual basis. Eligible residents must submit on an annual basis a valid Massachusetts Registry of Motor Vehicles registration and/or lease agreement, a valid Massachusetts driver's license, and current proof of residency as determined by the Department. Failure to re-qualify by the applicable expiration date will result in the loss of the resident toll rate. While not in the program, the subject resident shall be responsible for the full toll rate and the full, non discounted toll rate will be posted to the subject E-ZPass MA account or invoiced as a Pay By Plate toll transaction.

St. 1995, c. 102, § 14 was enacted as a mitigation measure resulting from construction activities of the Central Artery/Tunnel Project and the increased amount of traffic passing through the affected communities of East Boston, the North End of Boston, and South Boston. In order to mitigate the impacts of construction and traffic on certain sections of the city of Boston most directly affected, St. 1995, c. 102, § 14 was enacted which states in pertinent part that the Department may not charge and collect tolls for transit through the Callahan tunnel, the Sumner tunnel or the Third Harbor tunnel by private passenger vehicles registered in the East Boston or South Boston sections of the city of Boston, that are greater than the tolls in effect for such vehicles at existing tunnel toll facilities on August 10, 1995; and further, that the Department may not charge and collect tolls for transit through the Callahan or Sumner tunnels to private passenger vehicles registered in the North End section of the city of Boston, that are greater than the tolls in effect for such transit through either the Sumner tunnel or Callahan tunnel for such vehicles on August 10, 1995.

(8) E-ZPass MA Requirement Two Axle Commercial Vehicles and Common Carriers.

(a) Two Axle Commercial Vehicles. All two axle Commercial Vehicles, as defined in 700 CMR 7.02, operating through the Sumner Tunnel, Callahan Tunnel, and/or the Ted Williams Tunnel in Boston, Massachusetts, shall be equipped with an E-ZPass MA device, as described within the provisions of 700 CMR 7.04, for the payment of the required toll in accordance with the appropriate vehicle classification contained in 700 CMR 7.03(9)(a).

(b) Common Carriers. All Common Carriers, as defined in M.G.L. c. 159A, operating on any way under the jurisdiction of the Department for which operation said Common Carrier must obtain a Common Carrier License from the Department in accordance with M.G.L. c. 159A, shall be equipped with an E-ZPass MA device, as described within the provisions of 700 CMR 7.04, for the payment of the required toll in accordance with the appropriate vehicle classification contained in 700 CMR 7.03(9)(b).

7.04: EZDriveMA Toll Collection

(1) EZDriveMA System. The Department from time to time establishes the terms and conditions governing the use of the E-ZDrive MA system and requires that all users of the EZDriveMA System accept these terms and conditions. The EZDriveMA system is comprised of E-ZPass MA and Pay By Plate.

(2) Use of the EZDriveMA System. No person may use or attempt to use the Department's EZDriveMA system unless:

(a) the vehicle driven is properly registered with the appropriate RMV/DMV;

(b) the vehicle license plate number, jurisdiction, and other identifying characters on the license plate are all clearly visible at all times and the license plate(s) is/are unobstructed and mounted in compliance with M.G.L. c. 90, § 6; and

(c) the person agrees to adhere to all laws, regulations and terms and conditions governing the use of the Massachusetts Turnpike, MHS and the EZDriveMA system.

(3) E-ZPass MA Account and Use of On the Go Device. No person may possess an electronic device for use with the EZDriveMA system unless:

(a) the person is duly registered with the Department or its designated EZDriveMA contractor as an Account Holder; or

7.04: continued

(b) the person is operating an authorized E-ZPass MA equipped Motor Vehicle with the permission of the Account Holder of the E-ZPass MA equipped Motor Vehicle; and
(c) the person has a valid OTG device and is using MassDOT facilities in accordance with applicable regulations and terms and conditions; or
(d) the person is using a valid electronic device of an electronic toll collection system of another jurisdiction that maintains reciprocity with the Department; and
(e) the person is operating a valid E-ZPass MA-equipped Motor Vehicle and that device is properly programmed to assess the appropriate toll charge as determined by the Department from time to time, for the classification of the vehicle that is using the E-ZPass MA System in accordance with the classification of that vehicle enumerated in 700 CMR 7.03;
(f) the vehicle is properly registered with the appropriate RMV/DMV; and
(g) the electronic device is properly mounted and operable and the associated account is in good standing.

(4) Pay By Plate Program. Driving on a MassDOT toll roadway without an E-ZPass MA account, Pay By Plate Registered account, or a toll account of another agency that has toll reciprocity with MassDOT, will result in an invoice issued to the registered owner or responsible party, where applicable, based on an image taken of the vehicle license plate or other identifying information. Pay By Plate invoices and notices will be issued according to the following processes:

(a) Pay By Plate Invoice is an itemized statement issued to the vehicle's registered owner of record, or other responsible party, where applicable, in accordance with 700 CMR 7.02. The Registered Owner or responsible party must pay the Balance Due by the Payment Due Date on the Pay By Plate Invoice.
(b) Pay By Plate Past Due Invoice is an itemized statement issued to the vehicle's registered owner of record, or other responsible party, in accordance with 700 CMR 7.02 The Balance Due must be received by MassDOT by the Payment Due Date on the Pay By Plate Past Due Invoice. Late fees, fines, or other penalties may be assessed when any portion of the Balance Due from the Pay By Plate Invoice is outstanding after the Pay By Plate Invoice Payment Due Date.
(c) Pay By Plate Notice of Non Payment (NONP) is an itemized statement issued to the vehicle's registered owner of record, or other responsible party, where applicable, in accordance with 700 CMR 7.02 The Balance Due must be received by MassDOT by the Payment Due Date on the Pay By Plate NONP. Late fees, fines, or other penalties may be assessed when any portion of the Balance Due from the Pay By Plate Past Due Invoice is outstanding after the Pay By Plate Past Due Invoice Payment Due Date.
(d) Pay By Plate Notice of Liability (NOL) is an itemized statement issued to the vehicle's registered owner of record, or other responsible party, where applicable, in accordance with 700 CMR 7.02. Late fees, fines, or other penalties may be assessed when any portion of the Balance Due from the Pay By Plate NONP is outstanding after the Pay By Plate NONP Payment Due Date. The Registered Owner must pay the NOL Balance Due immediately. The issuance of an NOL constitutes notification that enforcement action with the RMV/DMV has been taken in accordance with 700 CMR 7.05(4).
(e) MassDOT may assess a higher toll rate or other fee to a Pay By Plate customer, for the costs associated with administering the Pay By Plate program.

(5) Unauthorized Use. Only customers in good standing who comply with applicable terms and conditions and rules and regulations are authorized to use the EZDriveMA system. A person who operates a motor vehicle which is not an authorized E-ZPass MA equipped Motor Vehicle, listed on a Pay By Plate Registered account, or using an electronic toll collection device of another agency or entity that has toll collection reciprocity with MassDOT, shall be considered a Pay By Plate customer and shall be subject to the provisions of 700 CMR 7.04. A person who has been issued a Notice of Liability for failure to pay one or more Pay By Plate invoices, and said invoices remain unpaid, shall not be authorized to use the EZDriveMA system.

(6) Assessment of Toll. A motor vehicle that travels on the tolled portions of the Massachusetts Turnpike and/or the MHS will incur a toll. The Department assesses the appropriate toll charge against the corresponding E-ZPass MA Account Holder or for Pay By Plate account to the Registered Owner of record of the vehicle or responsible party, where applicable.

7.04: continued

(7) Evasion of Toll by Device or Method. No person may use or attempt to use any device or method, the intended result of which is the inability of the EZDriveMA system to assess or collect the toll due under 700 CMR 7.03 or the non payment of the toll. Failure to comply with 700 CMR 7.04(7) shall be considered toll evasion and/or unauthorized use of the EZDriveMA system.

(8) *Prima Facie* Responsibility. The registered owner of record of the motor vehicle is *prima facie* responsible for the payment of the tolls, fees, fines and/or penalties that the Department assesses with respect to the nonpayment of the toll unless:

(a) Stolen Vehicle. The registered owner of record has reported in a timely manner to a police agency that the subject vehicle has been stolen, and the subject vehicle remained stolen at the time of the toll transaction; or

(b) Leased or Rented Vehicle. The registered owner of record is in the business of leasing or renting motor vehicles and provides to MassDOT by the Payment Due Date on the Pay By Plate invoice, a copy of a lease, rental or similar contract document indicating that the vehicle was leased or rented at the time of the toll transaction and the identity, address and driver's license information of the person entitled to possession is discernible from the document, in which case that person is *prima facie* responsible for the payment of the fines or penalties that the Department assesses in accordance with 700 CMR 7.00.

(9) Toll Rate Discount. Pay By Plate customers and non-EZDriveMA customers shall not be eligible for the toll discount program provided for in M.G.L. c. 6C, § 13(b), Toll rate discounts shall only be available to two-axle passenger vehicles listed on passenger E-ZPass MA accounts.

7.05: EZDriveMA Toll Enforcement

(1) Enforcement. Operators who use the EZDriveMA system acknowledge and authorize MassDOT or its contractor to acquire the name and address of the Registered Owner of record of the vehicle for purposes of EZDriveMA toll collection and enforcement. A Clerk may enforce the provisions of 700 CMR 7.05.

(2) Designation of Clerks. MassDOT may designate one or more Clerks to perform the functions specified in 700 CMR 7.05(3) for MassDOT and for such finite or indefinite period as MassDOT deems desirable.

(3) Functions of the Clerks. The Clerks coordinate and administer the processing of EZDriveMA statements, invoices and notices, and any and all other duties and tasks associated with toll collection, toll enforcement, and the EZDriveMA system. MassDOT may hire or designate such personnel and organize such divisions as MassDOT may deem necessary, or contract for such services, in order to carry out the provisions of 700 CMR 7.05(3).

(4) Issuance and Content of Pay By Plate Invoices and Notices.

(a) Information Regarding the Balance Due. A Pay By Plate Invoice and notice include, but is not limited to, the following information: the registration number and state of issuance of the registration number of the vehicle involved; the name of the registered owner of the vehicle, or other responsible party where applicable; the lessee or renter as identified by 700 CMR 7.04(8)(b); the date, time and place of the transaction; the total amount owed; the applicable fines or penalties incurred that MassDOT has assessed; and such other information as MassDOT may deem appropriate.

(b) Notice of Requirement to Respond. A Pay By Plate invoice and notice states that the Registered Owner of record or responsible party where applicable, must pay the Balance Due by the Payment Due Date, appeal, or request a hearing for these items. The invoice and notice describes the means and content of the response for payment or appeal.

7.05: continued

(c) Delivery of Invoice and Notice. A Clerk issues and may certify invoices and notices as soon as practicable by mail to the Registered Owner of the vehicle or responsible party, where applicable at the address of the registrant on record with the Massachusetts Registry of Motor Vehicles, or, in the case of a motor vehicle registered under the laws of another state or jurisdiction, at the address of the registrant on record with the official in the state or other jurisdiction having charge of the registration of the vehicle, or as supplied by a third party provider under contract with the Department, or to the name and address of the lessee or renter in accordance with 700 CMR 7.04(8)(b). Notices of Liability shall be sent to the Registered Owner of the vehicle.

(d) *Prima Facie* Evidence of Notice. Delivery by mail of a copy of an Invoice or Notice is sufficient notice of the failure to pay the required toll and/or Balance Due. Certification of the invoice or notice by a Clerk is *prima facie* evidence of the facts contained therein and is admissible in any administrative or judicial proceeding to adjudicate the liability for the unpaid toll transactions, and related fees, fines and penalties. The Clerk shall maintain a docket of all copies of notices.

(5) Payment of Balance Due or Appeal. The Registered Owner of record or responsible party, where applicable, shall pay all tolls, fines, fees, and penalties that may be assessed by MassDOT by the Payment Due Date on the invoice or notice, or appeal in accordance with the procedures in 700 CMR 7.05.

(a) Payment. The registered owner or responsible party, where applicable, shall pay the tolls, fines, fees and penalties that may be assessed by MassDOT by the Payment Due Date as specified in the invoice and notice. Failure to do so may result in additional fees, fines and penalties.

(b) Appeal by Mail. The registered owner or responsible party, where applicable, may, without waiving the right to a hearing before a Clerk as provided by 700 CMR 7.05(5)(c), and also without waiving judicial review as provided by M.G.L. c. 30A, § 14, appeal the assessment of a toll, fine, fee or other penalty and receive a review and disposition from a Clerk by mail. The appeal by mail must contain a signed statement from the registered owner or responsible party, where applicable, explaining the basis for the appeal. The signed statement may be accompanied by signed statements from witnesses, police officers, government officials, or other relevant parties or photographs, diagrams, maps or other relevant documents that the registered owner determines to submit. Statements or materials sent to a Clerk for review must have attached to them the name and address of the registered owner as well as the invoice number of the notice and the date of the invoice. All information submitted by the registered owner becomes part of the record. Written appeals submitted by mail must be received by MassDOT within 120 days of the date the charge first appears on the invoice or notice., The Clerk or other MassDOT designee shall, within 60 days of receipt of such material, review the material and dismiss or uphold the issuance of the notice and notify the registered owner or appellant of the disposition of the appeal in writing. If the appeal by mail is denied, the Clerk shall explain the reasons for the determination. The review and disposition handled by mail is informal, the rules of evidence do not apply, and the decision of the Clerk is final subject to the hearing provisions provided by 700 CMR 7.05(5)(c) and to judicial review as provided by M.G.L. c. 30A, § 14.

(c) Request for Hearing. Consistent with the provisions of M.G.L. c. 30A, a person issued a notice regarding the assessment of a toll, fine, fee or other penalty may make a written request for an appeal hearing before a Clerk designated by MassDOT. Requests for a hearing must be received by MassDOT within 30 days of the issuance of the decision of the appeal by mail pursuant to 700 CMR 7.05(5)(b), in order to be entitled to a hearing. The Clerk then notifies the Registered Owner or appellant in writing by mail of the date, time, and place of the hearing. The hearing is informal, the rules of evidence do not apply, and the decision of the Clerk is final, subject to judicial review as provided by M.G.L. c. 30A, § 14. Parties are notified in person or by mail of the decision following the hearing. Each written appeal decision contains a statement of reasons for the decision including a determination of each issue of fact necessary to the decision. Failure to appear at the date, time, and place specified on the hearing notice automatically results in the denial of the appeal.

7.05: continued

(d) The provisions of 700 CMR 7.05 do not apply to Uniform Traffic Citations issued by Massachusetts State Police officers pursuant to M.G.L. c. 90C. A violation of MassDOT's regulations that results in the issuance of a Uniform Traffic Citation by a Massachusetts State Police officer under M.G.L. c. 90C, is subject to the procedures that M.G.L. c. 90C provides.

(6) Failure to Comply. Failure to comply with the requirements of 700 CMR 7.05(5) shall result in the following sanctions against the registered owner.

(a) Additional Fines or Penalties. MassDOT assesses the following additional fines, fees or penalties for late payment, failure to pay, or for otherwise failing to respond to a notice as provided by 700 CMR 7.05(5), in accordance 700 CMR 7.05(6): *Table 2*. Fines, fees and penalties for unpaid tolls associated with use of EZDriveMA system shall not exceed $500.00 per year, per registered vehicle.

(b) Pay By Plate Past Due Invoice Late Fees. Failure to pay the Balance Due on the Pay By Plate Invoice may result in the issuance of a Pay By Plate Past Due Invoice. Each toll trip included on the Pay By Plate Past Due Invoice may be charged a late fee in accordance with 700 CMR 7.05(6): *Table 2*.

(c) Pay By Plate Notice of Non Payment (NONP) Late Fees. Failure to pay the Balance Due on the Pay By Plate Past Due Invoice may result in the issuance of a NONP. Each toll trip included on the NONP may be charged a late fee in accordance with 700 CMR 7.05(6): *Table 2*.

(d) Failure to Respond after Issuance of a Notice of Non Payment. A registered owner or other responsible party, where applicable, who fails to pay the tolls, fines, fees or other penalties as specified in the NONP, shall be assessed an RMV/DMV fee of $20.00 and the registered owner shall be issued a Notice of Liability. The Clerk notifies the registered owner by mail of this Notice of Liability and, in addition, notifies the Registrar of Motor Vehicles of MA or other states, where applicable, who shall place the matter on record and, the Registrar shall not renew the registered owner's license to operate a vehicle or the registration of the vehicle until after notice from the Clerk that all such matters have been disposed of in accordance with applicable law or regulation. If the registered owner is a resident of another state or jurisdiction, the Registrar shall revoke the registered owner's right to operate a motor vehicle in the Commonwealth until the matter has been disposed of in accordance with applicable law or regulation. The source of the Registered Owner information may be from the Registrar or similar official or department of another jurisdiction in accordance with the law of that jurisdiction or a third party service contracted by MassDOT for providing Registered Owner information, or from vehicle images that display information identifying the vehicle owner.

(e) Pay By Plate Notice of Liability (NOL) Late Fees. Failure to pay the Balance Due on the Pay By Plate NONP may result in the issuance of a NOL. Each toll trip included on the NOL may be charged a late fee in accordance with 700 CMR 7.05(6): *Table 2*.

TABLE 2

Invoice/Notice Issued	Days to Pay Invoice/Notice	Days Outstanding	Late Fees Assessed
1st Invoice Issued	30	1-30	$0
Past Due Invoice	30	31-60	$1.00 for each overdue toll charge
Notice of Non-payment	30	61-90	An additional $1.00 for each overdue toll charge
Notice of Liability	Due Immediately	>90	An additional $1.00 for each overdue toll charge; Plus a $20.00 RMV/DMV Fee

* MassDOT may charge a higher toll rate or other fee to Pay By Plate customers in accordance with 700 CMR 7.04(4)(e).

7.05: continued

(f) Civil or Criminal Action. MassDOT may pursue such civil or criminal action as it deems appropriate to collect outstanding tolls, fees, and fines assessed as well as such additional fines or penalties as MassDOT may assess in accordance with 700 CMR 7.00.

(7) Confidentiality of Records. MassDOT shall maintain the confidentiality of all information including, but not limited to, photographs or other recorded images and credit and account data relative to Account Holders who utilize its EZDriveMA toll collection system. MassDOT shall maintain procedures consistent with M.G.L. c. 66A. For purposes of 700 CMR 11.06(7), all EZDriveMA customers, including customers of another agency or entity that may have toll collection reciprocity with MassDOT, are considered Account Holders.

(8) Hot List Data. Notwithstanding any other law or regulation, data and information such as name, location, time and date of travel, regarding Hot List license plates and/or transponders, while such license plates and/or transponders are on the Hot List (Hot List Data), shall be made available to a representative of the Massachusetts State Police, designated by the Secretary of the Executive Office of Public Safety and Security (EOPSS). License plates and/or transponder numbers *shall only be included on the Hot List in limited 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 sufficient to necessitate the need to provide this Hot List Data to law enforcement. Such emergency situations shall include, but are not limited to terrorist threats, Amber Alerts, Silver Alerts, kidnappings, missing persons, and felons actively traveling to or from a crime scene.* The Secretary of EOPSS, or his or her designee, shall verify in writing which emergency situations warrant adding any license plate and/or transponder number to the Hot List. License plates and/or transponder numbers shall only remain on the Hot List for 14 days unless the Secretary of EOPSS or his or her designee certifies and justifies the need to maintain the numbers on the Hot List for a longer period, but in no event shall such numbers remain on the list longer than 30 days.

(9) System Maintenance and Enforcement. Any electronic or other automated system of toll collection used by MassDOT is regularly tested and maintained to promote accurate and efficient determinations as to payment or non-payment of tolls. Any invoice or notice based in whole or in part upon inspection of any photograph or other recorded image of a motor vehicle and the written certification by a Clerk shall be prima facie evidence of the facts contained therein and shall be admissible in any administrative or judicial proceeding to adjudicate the liability for such invoice or notice.

(10) Fines. Whoever violates any provision of 700 CMR 7.00 is subject to a fine not exceeding the amount indicated in 700 CMR 7.00 and below in addition to other penalties as the laws of Massachusetts or federal law may provide. The section and general subject matter headings are provided for convenience only and do not amend or in any way affect the substance of the provisions to which they refer.

7.06: Limitations on Use of Ways

(1) One-way Restriction. Lanes on a way are used for one-way traffic unless a sign specifically indicates that two-way traffic is permitted. An operator of a motor vehicle may not travel on a way contrary to the direction indicated or intended for travel unless a Massachusetts State Police officer or a sign directs the operator to do so.

(2) Use of the Callahan Tunnel and the Sumner Tunnel. An operator of a motor vehicle traveling from Boston to East Boston shall use the Callahan Tunnel and an operator of a motor vehicle traveling from East Boston to Boston shall use the Sumner Tunnel unless a toll collector, a Massachusetts State Police officer, or a sign directs the operator otherwise.

(3) Entry to and Exit from a Way. An operator may not cause a vehicle to enter or leave a way except through an interchange or other authorized point of entry or exit or at the direction of a Massachusetts State Police officer.

7.06: continued

(4) Prohibited Entry to or Use of a Way. The Department prohibits the following vehicles from entering or using a way:

(a) Improperly Seated. A vehicle carrying an individual who is not properly seated within the confines of the vehicle.

(b) Flat or Inadequate Tire. A vehicle with a flat, bald, unduly or unevenly worn, solid, or metal tire mounted on a wheel in contact with the roadway surface or with a tire mounted on a wheel in contact with the roadway surface that poses a risk to individuals or property or may render the use of the way unsafe by disintegrating or partially disintegrating during travel and distributing tire debris upon the way.

(c) Obstructed Window. A motor vehicle having a window or windshield obstructed in a manner prohibited by M.G.L. c. 90, § 9D.

(d) Propelled by Muscle Power. A vehicle propelled by muscle power, including without limitation a bicycle or a vehicle drawn by a horse or other animal, or a motorized bicycle or moped.

(e) Construction and Similar Equipment. A vehicle in contact with a way that has caterpillar treads or that is a type of construction, agricultural, or similar equipment not designed for or employed in general highway travel, whether designed to be self-propelled or towed.

(f) Falling Debris. A vehicle upon or in which snow, ice, or other unsecured or improperly secured article or material (debris) has gathered or been placed such that the debris may fall from the vehicle and endanger individuals or property or render the use of the way unsafe.

(g) Inadequate Brakes. A vehicle with inadequate brakes.

(h) Over-weight Vehicle. An over-weight vehicle, except under, and in accordance with the terms of, a special permit that the Department issues pursuant to 700 CMR 7.07(3)(b) or (c).

(i) Over-size Vehicle. An over-size vehicle, except under, and in accordance with the terms of, a special permit that the Department issues pursuant to 700 CMR 7.07(4)(b) or (c).

(j) Propelled by a Special Fuel in the Tunnels. A vehicle propelled by a special fuel while traveling in the Tunnels, except a vehicle propelled by compressed natural gas, or propane, provided the tunnel exhaust fans are in operation, and so long as the vehicle has a maximum fuel capacity consistent with safe practice and national standards, including Federal Motor Vehicle Safety Standards #303 and #304, and is equipped with excess flow valves for fuel lines with an inner diameter larger than ½ ", and is identified by a blue-and-white diamond decal attached as specified in NFPA 52, and is not used to transport compressed natural gas or propane.

(k) Carrying an Explosive. A vehicle carrying an explosive except pursuant to a special permit for explosives that the Department issues in accordance with 700 CMR 7.07(5).

(l) Carrying a Special Fuel. A vehicle, however propelled and whether or not carrying a special fuel, used to carry a special fuel, except under a special fuel transportation permit that the Department issues pursuant to 700 CMR 7.06(6).

(m) Carrying a Hazardous Material. A vehicle carrying a hazardous material except as 700 CMR 7.11 permits; provided that a vehicle may carry individual packages containing non-hazardous materials and carbon dioxide in solid or dry ice form for refrigeration purposes.

(n) Vehicles Posing Special Risks in Tunnels. A tandem unit except as 700 CMR 7.07(3)(c)4. permits; a passenger vehicle or commercial vehicle carrying cargo which may pose a risk to public safety; a passenger vehicle or commercial vehicle used for carrying any amount of hazardous materials; a passenger vehicle or commercial vehicle carrying hazardous materials in the form of consumer goods (consumer goods are those goods used or bought primarily for use by individuals for personal, family or household purposes); an empty tank vehicle or a vehicle transporting empty containers which were last used for the transportation of hazardous materials. Hazardous materials is defined and listed in 49 CFR Chapter 1, Subchapter C.

(o) Other Prohibited Vehicles. A vehicle emitting an offensive or obnoxious odor; a vehicle emitting an excessive amount of smoke; or a vehicle towed by chain, rope, or other non-rigid device.

(5) Pedestrians and Animals. No pedestrian may enter or use a way, and no person may allow a horse or other animal not properly contained in an appropriate vehicle to enter or use a way.

7.06: continued

(6) Aircraft. Aircraft are prohibited from landing on a way except in an emergency. No aircraft may take-off in flight from any portion of a way except with the written approval of the Chief Engineer and the Massachusetts State Police. Removal of an aircraft from a way by means other than take-off in flight requires the approval of the Massachusetts State Police.

(7) Hitchhiking and Loitering. No individual may engage in the solicitation of a ride, commonly known as "hitchhiking," on a way. An individual who, for the purpose of soliciting a ride on a way, displays a sign, signals a moving vehicle, causes the stopping of a vehicle, or stands on property of the Department in view of a ramp or roadway of a way, may be arrested without a warrant. No person may loiter in or about a way for the purpose of "hitchhiking" or for any other purpose.

(8) Commercial Activity - Solicitation of Funds. No person may carry on any commercial activity, except the transportation of individuals or property, without the written permission of, or unless under contract with, the Department. No person may post, distribute, or display signs, advertisements, circulars, or printed or written matter without the written permission of the Department. No person may solicit funds for any purpose without the written permission of the Department.

7.07: Special Limitations and Issuance of Special Permits

(1) Scope and Organization.

(a) Over-weight Vehicles; Over-size Vehicles; Small Tandem Units; and Vehicles Carrying Reducible Loads, Explosives, and Special Fuel. 700 CMR 7.07 establishes limitations on use and provides for special permits with respect to: over-weight vehicles, 700 CMR 7.07(3); vehicles carrying reducible loads, 700 CMR 7.07(3); small tandem units, 700 CMR 7.07(3)(c)4.; over-size vehicles, 700 CMR 7.07(4); vehicles carrying explosives, 700 CMR 7.07(5); and vehicles carrying a special fuel, 700 CMR 7.07(6).

(b) Applicability to Large Tandem Units. The provisions of 700 CMR 7.07 apply to large tandem units except that 700 CMR 7.08(3) and (4) governing length and weight limitations, respectively, applicable to large tandem units, supersede any conflicting provisions of 700 CMR 7.07.

(2) Practices and Procedures Regarding Special Permits.

(a) Application to the Department. An owner or operator (applicant) may apply to the Department for a special permit on a written form (application) that the Department provides for this purpose. The Chief Engineer may approve an application on those terms or conditions, if any, as the Chief Engineer determines are consistent with the safe and efficient operation of the way over which permission to travel is sought. The Department accepts applications mailed or delivered to the office of the Chief Engineer and may, at its discretion, accept applications by facsimile transmission.

(b) Payment of Fees. An applicant must pay the fees that are specified in the application and in 700 CMR 7.07(3)(c)3.: *Table 5*. The Department specifies on the application the time and manner of payment.

(c) Approval or Disapproval. The Department notifies the applicant of the approval or disapproval of the application as soon as is reasonably practicable and in a manner specified on the application.

(d) Discretion of the Department. The Department may at any time decline to issue, with or without a prior hearing as it determines, any special permit. The Department may at any time suspend or revoke a special permit. The Department provides a hearing with respect to any such decision in the manner and to the extent required by law.

(e) Effect of Misrepresentation. A material misrepresentation as to the weight or the dimensions of a vehicle or its load, or the nature of the load, that an applicant or the applicant's agent, employee, or lessee makes to the Department voids the special permit under which the vehicle is operating. A Massachusetts State Police officer or an authorized employee of the Department may verify at any time the weight, dimensions, or load of a vehicle.

(f) Not Transferable. A special permit is valid only for the vehicle or vehicles that the Department approves in the special permit and is not transferable to another vehicle.

7.07: continued

(g) Emergency Suspension. The Department, acting by the responsible commanding officer of the Massachusetts State Police or, in the absence of the commanding officer, the officer's designee, may suspend the use of a special permit when road or weather conditions or the volume of traffic warrant doing so, as the commanding officer or designee determines.

(h) Restrictions on Irreducible Load Permits. An irreducible load permit is valid for a trip in one direction through one of the Tunnels or between specified interchanges on the Turnpike unless the permit specifies otherwise. The Department may restrict travel under an irreducible load permit to specified days or hours. The Department ordinarily does not issue an irreducible load permit for travel in the Sumner Tunnel or the Ted Williams Tunnel in the direction away from Logan Airport between 7:00 A.M. and 10:00 A.M. or in the Callahan Tunnel or Ted Williams Tunnel in the direction toward Logan airport between 3:00 P.M. and 7:00 P.M. The Department ordinarily does not issue an irreducible load permit for travel on the Turnpike between Interchange 11A in Westborough and Interchange 24 in Boston eastbound between 7:00 A.M. and 10:00 A.M. or westbound between 3:00 P.M. and 7:00 P.M.

(i) No Representation. The Department's issuance of a special permit does not constitute a representation by the Department of the adequacy of the way to support or accommodate the passage of a special permit vehicle with its load.

(j) Applicant's Responsibility. An applicant is responsible for injury to, or the death of, individuals and for damage to the Department or public or private property resulting directly or indirectly from the presence on a way of a special permit vehicle or its operation by the applicant, whether owner or lessee, or by the applicant's agents, employees, or contractors. By applying for and using a special permit, an applicant agrees to save the Department, its members, officers, and employees harmless from liability for any such injury, death, or damage. The Department requires that an applicant agree to indemnify the Department against damage or injury resulting from the operation of the special permit vehicle on the way and to maintain such insurance as the Department considers appropriate as specified in the application. By submitting an application for a special permit, an applicant agrees to these requirements and certifies that the required insurance is in force.

(k) Demonstration of Need for Irreducible Load Permit. An applicant for an irreducible load permit must demonstrate the number of work hours required to dismantle the load.

(l) Circumstances under Which a Special Permit Is Not Issued. The Department does not issue a special permit with respect to weight, and a vehicle may not use a way, if the vehicle weight exceeds the gross vehicle weight rating or the gross weight for which the vehicle is registered, except that the Department may issue a special permit for a vehicle having a vehicle weight in excess of its registered gross weight if it is owned or leased by a carrier that is not domiciled in the Commonwealth of Massachusetts.

(m) Tandem Units Not Permitted in the Tunnels. Except as provided in 700 CMR 7.07(3)(c)4. and notwithstanding any other provision of 700 CMR 7.07 to the contrary, tandem units are not permitted in the Tunnels.

(3) Limitations on Weight.

(a) Circumstances under Which No Special Permit Is Required. A vehicle does not require a special permit with respect to its weight if the vehicle weight does not exceed the maximum vehicle weight indicated in 700 CMR 7.07(3): *Table 2* for a vehicle of its type, except that a special permit may nonetheless be required in accordance with the provisions of 700 CMR 7.07(3)(b)2. or 3. A vehicle may not use a way if its vehicle weight does not conform to the requirements of 700 CMR 7.07.

TABLE 3

Type of Vehicle	Maximum Vehicle Weight
Motor Vehicle with two axles	46,000 lbs.
Vehicle or vehicle combination with three axles	73,000 lbs.
Vehicle or vehicle combination with four or more axles	87,000 lbs.
Vehicle or vehicle combination with five or more axles	99,000 lbs.

7.07: continued

(b) Circumstances under Which a Special Permit Is Required. A motor vehicle, vehicle, or vehicle combination requires a special permit if:

1. the vehicle weight exceeds the maximum vehicle weight as indicated in 700 CMR 7.07(3)(a): *Table 3*; or

2. the weight on any axle, measured at the ground, exceeds the maximum weight indicated in 700 CMR 7.07(3): *Table 4* for the applicable spacing between axles of the vehicle;

TABLE 4

Axle Spacing	Maximum Weight
A single axle or axles spaced less than six feet apart	18,000 lbs.
Axles spaced six feet or more apart	22,400 lbs.

or,

3. the overall gross weight on a group of two or more consecutive axles exceeds 80,000 pounds or the value of "W" produced by application of the Bridge Gross Weight Formula, whichever is less, except that two consecutive sets of tandem axles may carry a gross load of 34,000 pounds each, provided that the overall distance between the first and last axles of the consecutive sets of tandem axles is 36 feet or more.

Bridge Gross Weight Formula:

$W = 500 (LN/N-1 + 12N + 36)$

where:

"W" represents the overall gross weight in pounds on any group of two or more consecutive Axles to the nearest 500 pounds,

"L" represents the distance in feet between the extreme of any group of two or more consecutive Axles, and

"N" represents the number of Axles in the group under consideration.

(c) Types of Special Permits Issued (Over-weight and Small Tandem Units). The Department issues special permits for over-weight vehicles in accordance with the following provisions:

1. Irreducible Load Permit. The Department may issue an irreducible load permit for over-weight vehicles in accordance with the procedures and subject to the terms of 700 CMR 7.07(2) and subject to 700 CMR 7.07(2)(1) for vehicles weighing more than the maximum vehicle weight indicated in 700 CMR 7.07(3): *Table 3*, upon the approval of the Chief Engineer. The applicant must pay the fees that are specified in the permit application and in 700 CMR 7.07: *Table 5* and the toll charge based on the classification of the vehicle, under 700 CMR 7.03(1). In the case of an annual permit, multiple trips of a single vehicle or a convoy of vehicles, the fee specified on the permit application represents the total fee due up to a maximum number of trips of two or more as determined by the Chief Engineer, provided that the applicant specifies on the application referred to in 700 CMR 7.07(2)(a) the number of anticipated multiple trips, the time period in which they will be completed, and other information that the application or the Chief Engineer require.

2. Use of the Ted Williams Tunnel, Including the South Boston Bypass Road. A vehicle weighing more than the maximum vehicle weight indicated in 700 CMR 7.07(3): *Table 3* requires an irreducible load permit for use of the Ted Williams Tunnel, including the South Boston Bypass Road, for construction equipment for the vehicle, allowing the vehicle to operate at a vehicle weight greater than that indicated in 700 CMR 7.07(3): *Table 3*. The operator of the vehicle is responsible for the regular toll charge based on the classification of the vehicle under 700 CMR 7.03(1).

7.07: continued

3. Reducible Load Permit. The Department issues a reducible load permit in accordance with the procedures and subject to the terms of 700 CMR 7.07(2) and subject to 700 CMR 7.07(2)(1) for vehicles weighing not more than the maximum vehicle weight indicated in 700 CMR 7.07(3): *Table 4.*

TABLE 5

Type of Permit	Fee
Irreducible Load Permit - Exceeding Any Legal Limit for Size and Weight Pursuant to 700 CMR 7.00	$400.00 - Annually for Travel on Turnpike and MHS
Irreducible Load Permit - Exceeding Any Legal Limit for Size and Weight Pursuant to 700 CMR 7.00	$40.00 Per Trip on Turnpike and MHS
Reducible Load Permit - Exceeding Any Legal Limit for Size and Weight Pursuant to 700 CMR 7.00	$50.00 per 1,000 pounds exceeding the Federal Bridge Formula
Tandem Trailer Permit	$300.00 Application Fee $75.00 for First Card $25.00 for Each Additional Card
Explosives Permit	$300.00 Application Fee $75.00 for First Card $25.00 for Each Additional Card
Special Fuel Hauling	$300.00 Application Fee $75.00 for First Card $25.00 for Each Additional Card
Super Load Weight >130,000 pounds - Detailed Engineering Calculations Required	$300.00 Single Trip on Turnpike and MHS

TABLE 6

Type of Vehicle	Maximum Vehicle Weight
Vehicle or vehicle combination with three axles	73,000 lbs.
Vehicle or vehicle combination with four axles	87,000 lbs.
Vehicle or vehicle combination with five or more axles	99,000 lbs.

A reducible load permit issued to an owner or lessee may be used in connection with a valid sticker issued by the Registrar of Motor Vehicles in accordance with M.G.L. c. 90, § 19D. An original reducible load permit must be kept in an accessible place in the vehicle for which it was issued and must be presented to a toll collector, other official or employee of the Department, or Massachusetts State Police officer on demand. A copy of the original is not an acceptable substitute. In enforcing compliance with 700 CMR 7.07(3)(c)2. the Department provides an allowance of 5% above the maximum vehicle weights specified in 700 CMR 7.07(3): Table 6, rounded to the nearest 500 pounds. For example, a vehicle with five or more axles is deemed to be in compliance with the weight requirement of its reducible load permit provided that the vehicle and its load weighs not more than 105% of 99,000 pounds or 104,000 pounds.

7.07: continued

The applicant must pay the non-refundable fee that is specified on the permit application and in 700 CMR 7.07(3): *Table 5*. Upon application and payment of this fee, the Department issues the number of reducible load permits as the owner or lessee may request for the vehicles of the owner. The fee for a reducible load permit is in addition to the regular toll charge based on the classification of the vehicle under 700 CMR 7.03(1).

4. Small Tandem Unit Permit. The Department may issue a special permit for small tandem units in accordance with the procedures and subject to the terms of 700 CMR 7.07(2). An operator may operate a small tandem unit in the Prudential Tunnel and portions of the Seaport Access Tunnel (I-90 Connector Tunnel) in accordance with the conditions contained in said permit, only if the Department has issued a small tandem unit permit or any renewal thereof pursuant to 700 CMR 7.07 and the permit and any renewal thereof has not expired or been revoked.

The applicant must pay the fee that is specified on the permit application and in 700 CMR 7.07(3): *Table 5*. The fee is in addition to the regular toll charge based on the classification of the vehicle under 700 CMR 7.03(1).

An original annual permit for small tandem units must be kept in an accessible place in the vehicle for which it was issued and must be presented to a toll collector, other official or employee of the Department, or Massachusetts State Police officer on demand. The operator of the vehicle is responsible for the regular toll charge based on the classification of the vehicle under 700 CMR 7.03(1).

(4) Limitations on Size.

(a) Circumstances under Which No Special Permit Is Required. A vehicle does not require a special permit with respect to its size if the vehicle does not exceed any of the applicable maximum dimensions specified in 700 CMR 7.07(4)(a)1., 2., or 3.

1. Width. The vehicle width is no greater than eight feet, six inches for use of the Tunnels and the vehicle width is no greater than eight feet, six inches for use of a way other than the Tunnels.

2. Height. The vehicle height is no greater than the maximum vehicle height for the way upon which the vehicle is traveling as indicated in 700 CMR 7.07(4): *Table 7*.

TABLE 7

Way	Maximum Vehicle Height
Turnpike	13 feet 6 inches
Ted Williams Tunnel	13 feet 6 inches
Callahan Tunnel	12 feet 6 inches
Sumner Tunnel	12 feet 6 inches
Thomas P. O'Neill, Jr., Tunnel	13 feet 6 inches
Prudential Tunnel	13 feet 6 inches
CANA (City Square) Tunnels	13 feet 6 inches
Other Way Not Listed Above	13 feet 6 inches

3. Length. For use of the Tunnels, the vehicle length is no greater than the maximum vehicle length for a vehicle of its type as indicated in 700 CMR 7.07(4): *Table 8* and, in the case of a tandem unit operating on a way, as indicated in Note 4 to 700 CMR 7.07(4): *Table 8*. For use of a way other than the Tunnels, the vehicle length is no greater than 55 feet for a vehicle with more than two axles, except a bus; the vehicle length is no greater than 45 feet for a bus; and the vehicle length is no greater than 100 feet for a vehicle combination, except a vehicle combination listed in 700 CMR 7.06(4): *Table 8* and a vehicle subject to 700 CMR 7.08.

7.07: continued

TABLE 8

Type of Vehicle	Maximum Vehicle Length
Motor vehicle not of the type listed below in 700 CMR 7.07(4): *Table 8*	33 feet
Vehicle combination other than semi-trailer unit and not of a combination type listed below in 700 CMR 7.07(4): *Table 8*	60 feet (see note 1)
Articulated Bus	60 feet
Auto Home	40 feet
Automobile Transporter (traditional)	65 feet (*see* Note 2)
Automobile Transporter (stinger-steered)	75 feet (*see* Note 2)
Boat Transporter (traditional)	65 feet (*see* Note 2)
Boat Transporter (truck-trailer)	65 feet (*see* Note 2)
Boat Transporter (stinger-steered)	75 feet (*see* Note 2)
Bus or School Bus	45 feet
House Trailer	40 feet
Saddlemount Combination	75 feet (see Note 3)
Semi-trailer	53 feet
Tandem unit	(see Note 4)
Trailer in tractor-trailer combination	53 feet
Trailer not in tractor-trailer combination	33 feet
Truck	40 feet

Note 1: No overall length limitation applies to a semi-trailer unit with a semi-trailer up to 53 feet in length. For purposes of 700 CMR 7.07(4): *Table 8*, the combination of a motor vehicle designed for towing and a vehicle or combination of vehicles being towed because of disablement or emergency does not constitute a vehicle combination and thus is not subject as a vehicle combination to the length limitations of 700 CMR 7.07(4)(a)3., but a Massachusetts State Police officer or an official of the Department designated to make such decisions may preclude such a towing motor vehicle and towed vehicle or vehicle combination from using a way for reasons of safety.

Note 2: The vehicle length includes front and rear bumpers, but does not include a load overhang up to three feet beyond the foremost part of the front transporting vehicle or more than four feet beyond the rear bed of the rear vehicle.

Note 3: A number of vehicles may be transported in combination by means of saddlemount combination or fullmount mechanism. Vehicles using these mechanisms must conform to M.G.L. c. 90, § 19C.

Note 4: Subject to the restrictions that 700 CMR 7.07(4)(e) and 7.08 impose, a tandem unit may operate on a way without a special permit with respect to its length, provided that:

1. the overall total number of semi-trailers or trailers in the tandem unit is no greater than two;
2. each semi-trailer or trailer of the tandem unit does not exceed 28 feet in length, without regard to the overall length of the tandem unit; and
3. a tandem unit with semi-trailers or trailers that do not exceed 28½ feet in length, if such semi-trailers or trailers were actually and lawfully operating on December 1, 1982, as part of tandem units within a 65 foot overall length limit in any state, may similarly operate on a way without a special permit with respect to its length.

7.07: continued

(b) Circumstances under Which a Special Permit Is Required. A motor vehicle, vehicle, or vehicle combination requires a special permit with respect to its size only when compliance with the maximum size limitations specified in 700 CMR 7.07(4)(a)1., 2., or 3. is impossible or impractical.

(c) Type of Special Permit Issued (Over-size). The Department issues special permits for over-size vehicles in accordance with the following provisions:

1. Irreducible Load Permit. A vehicle requires an irreducible load permit if the vehicle width exceeds the maximum vehicle width permitted under 700 CMR 7.07(4)(a)1.; the vehicle height exceeds the maximum vehicle height permitted under 700 CMR 7.07(4)(a)2.; or, the vehicle length exceeds the maximum vehicle length allowed for a vehicle of its type as specified in 700 CMR 7.07(4)(a)3.

The Department does not issue an irreducible load permit if it believes that a load can be divided or arranged so as to conform with the limitations on its width, height, or length. The Department may prohibit an over-size vehicle from using a way if, in the opinion of the Chief Engineer, safety or the public convenience warrants the prohibition.

The Department may issue, upon the approval of the Chief Engineer, an irreducible load permit in accordance with the procedures and subject to the terms of 700 CMR 7.07(2) and (4)(f).

The applicant must pay the fee that is specified on the permit application and in 700 CMR 7.07(3): *Table 5*. This fee is in addition to the regular toll charge based on the classification of the vehicle under 700 CMR 7.03(1). In the case of multiple trips of a single vehicle or a convoy of vehicles, the fee represents the total fee due up to a maximum number of trips of two or more as determined by the Chief Engineer, provided that the applicant specifies on the application referred to in 700 CMR 7.07(2)(a) the number of anticipated multiple trips, the time period in which they will be completed, and any other information that the application or the Chief Engineer requires.

2. Use of the Ted Williams Tunnel, Including the South Boston Bypass Road. A vehicle that exceeds any of the applicable maximum dimensions specified in 700 CMR 7.07(4)(a)1., 2., or 3. requires an irreducible load permit for use of the Ted Williams Tunnel, including the South Boston Bypass Road for construction equipment. An original annual permit for construction equipment issued by the Department must be kept in an accessible place in the vehicle for which it was issued and must be presented to a toll collector, other official or employee of the Department, or Massachusetts State Police officer on demand. The operator of the vehicle is responsible for the regular toll charge based on the classification of the vehicle under 700 CMR 7.03(1).

(d) Pilot Car.

1. When Required. A pilot car must follow an over-size vehicle if: the overhang is four or more feet and the load consists of poles, masts, booms, or similar shapes or if the overhang is ten feet or more; the over-size vehicle is a drill rig with boom, a shovel, or a crane; the over-size vehicle is odd-shaped or has an odd-shaped load; or the over-size vehicle is not a tandem unit or a semi-trailer unit with a semi-trailer of not more than 53 feet and has a length of more than 80 feet and less than 95 feet or a width of more than 12 feet.

2. Convoy Pilot Car. If two or more over-size vehicles are in convoy, one may be pilot for the other, but a separate pilot car must follow the last over-size vehicle.

3. Preceding and Following Pilot Cars. If an over-size vehicle is not a tandem unit or a semi-trailer unit with a semi-trailer of not more than 53 feet and has a length of more than 95 feet or width of more than 13 feet, it must have pilot cars preceding and following it.

4. Requirements for a Pilot Car. A pilot car must be a truck with two axles and four wheels or a private passenger motor vehicle and must have two flashing amber lights visible from front and rear; 24 inch by 24 inch red flags on the right and left rear of the pilot car; and a sign reading: "Oversize Load."

5. State Police Escort. In addition to the requirements with respect to a pilot car as specified in 700 CMR 7.07(4)(d), an over-size vehicle, with its load, that is wider than 15 feet or longer than 135 feet must be escorted by two motor vehicles of the Massachusetts State Police. Any vehicle that, in the opinion of t he Chief Engineer, may be incapable of operating at a minimum speed such that it may pose a danger to individuals, property, or the safe operation of a way, may be required to be accompanied by motor vehicles of the Massachusetts State Police.

7.07: continued

6. Oversize Load Sign. An oversize vehicle that is not required to be accompanied by a pilot car must have a sign on the rear reading: "Oversize Load."

(e) Tandem Units and Certain Saddlemount Combinations Not Permitted in the Tunnels. Subject to 700 CMR 7.07(3)(c)4., and notwithstanding any other provision of 700 CMR 7.07 to the contrary, and irrespective of their length, tandem units, double saddlemount combinations, and triple saddlemount combinations are not permitted in the Tunnels.

(f) Height Indication. No vehicle that has a total height exceeding ten feet, excluding the height of its load, may be operated on a way unless the measurement of the total height is painted or printed in letters and numerals at least four inches high in a conspicuous place upon the side or front of the vehicle.

(g) Responsibility of Operator. The operator of an over-size vehicle is responsible for checking the clearance of the vehicle and its load through any toll lane or canopy and for checking structures on a way for available clearance with respect to movements by the oversize vehicle or by load movements. The operator is subject to the penalty provided in 700 CMR 7.13(3)(a) for failure to exercise this care. The Department imposes this penalty in addition to holding the operator liable for the damage resulting from failure to exercise this care.

(5) Limitations on the Transportation of Explosives.

(a) General Prohibition. No vehicle carrying explosives may enter or use a way unless specifically allowed to do so by a provision of 700 CMR 7.07(5) and only to the extent and upon the conditions so specified. Any specific prohibitions contained in other subsections of 700 CMR 7.07(5) do not limit the generality of 700 CMR 7.07(5)(a).

(b) Operation Prohibited in Tunnels. No vehicle carrying explosives may enter or use the Tunnels.

(c) Operation Prohibited on Ways Other than the Tunnels. No vehicle carrying explosives may enter or use the Turnpike at or between Interchange 15 in Weston and Interchange 24 in Boston.

(d) No Liquid Nitroglycerin. No vehicle carrying liquid nitroglycerin may enter or use a way.

(e) Ways upon Which Department May Issue Permit. No vehicle used to carry explosives may enter and use the Turnpike at or between Interchange 1 in West Stockbridge and Interchange 14 in Weston unless the Department has issued for the vehicle a special permit for explosives as provided in 700 CMR 7.07(5)(f) and the vehicle and its operation fully comply with those provisions, except that a vehicle carrying no explosives other than fireworks not in excess of ten pounds, or other than 1,000 blasting caps or fewer, may enter and use that portion of the Turnpike without obtaining a special permit for explosives.

(f) Special Permit for Explosives.

1. Application. An owner or operator of a vehicle who has determined to obtain a special permit for explosives may apply for one in accordance with and subject to the provisions of 700 CMR 7.07(2). Among other information required by the application, the applicant shall indicate the number of vehicles to be covered under the application.

2. Terms and Conditions. The Department may issue a special permit for explosives for any 12 month period, together with a separate certification card for each vehicle enumerated in the permit application, as evidence that the vehicle is covered by the permit, subject to the following terms and conditions: a vehicle for which the Department has issued a special permit for explosives and certification card may make an unlimited number of trips on a way in accordance with 700 CMR 7.07(5)(e) or a portion of a way as designated on the permit or certification card; the operator of the vehicle must carry an original, not a copy, of the certification card in an accessible place and must display it to a toll collector, other official or employee of the Department, or Massachusetts State Police officer on demand.

3. Fees. The applicant must pay the fee that is specified on the permit application and in 700 CMR 7.07(3): *Table 5*. The applicant shall also pay the fee for the first certification card referred to in 700 CMR 7.07(5)(f)2. and an additional fee for each additional certification card that the Department issues during the term of the permit. The applicant must submit with its application full payment for the application fee and for all additional fees for the number of vehicles specified in the application. All these fees are in addition to any regular toll charge that the Department assesses in accordance with 700 CMR 7.03.

7.07: continued

4. Minimum Separation of Vehicles. No vehicle carrying explosives may operate within 1,000 feet longitudinally of another vehicle carrying explosives or any vehicle transporting hazardous material as defined in 49 CFR Chapter I, Subchapter C.

5. No Stopping. No vehicle carrying explosives may stop on a way, including a service or rest area, unless the movement of the vehicle is obstructed; it is disabled; or the operator of the vehicle is following the directions or requirements of a Massachusetts State Police officer, a sign, or governing federal regulations.

6. Conformance with Law. The equipment, cargo, operator, and operation of a vehicle operating under a special permit for explosives must conform with all federal and state laws and regulations governing the transportation of explosive materials by a motor carrier.

(6) Limitations on the Transportation of Special Fuels.

(a) General Prohibition. No vehicle used to carry a special fuel, however propelled and whether or not containing a special fuel, may enter or use a way unless specifically allowed to do so by a provision of 700 CMR 7.07(6) and only to the extent and upon the conditions so specified. Any specific prohibitions contained in other subsections of 700 CMR 7.07(6) do not limit the generality of 700 CMR 7.07(6)(a).

(b) Operation Prohibited in Tunnels. No vehicle used to carry a special fuel, however propelled and whether or not containing a special fuel, may enter or use the Tunnels.

(c) Operation Prohibited on Ways other than the Tunnels. No vehicle used to carry a special fuel, however propelled and whether or not containing a special fuel, may enter or use the Turnpike at or between Interchange 15 in Weston and Interchange 24 in Boston.

(d) Ways upon Which Department May Issue Permit. No vehicle used to carry a special fuel, however propelled and whether or not containing a special fuel, may enter and use the Turnpike at or between Interchange 1 in West Stockbridge and Interchange 14 in Weston unless the Department has issued for the vehicle a special fuel transportation permit as provided in 700 CMR 7.07(6)(e) and the vehicle and its operation fully comply with those provisions.

(e) Special Fuel Transportation Permit.

1. Application. An owner or operator of a vehicle who has determined to obtain a special fuel transportation permit may apply for one in accordance with and subject to the provisions of 700 CMR 7.07(2). Among other information required by the application, the applicant shall indicate the number of vehicles to be covered under the application.

2. Terms and Conditions. The Department may issue a special fuel transportation permit for any 12 month period for the type of special fuel or fuels the Department designates on the permit application, together with a separate certification card for each vehicle enumerated in the permit application, as evidence that the vehicle is covered by the permit, subject to the following terms and conditions: a vehicle for which the Department has issued a special fuel transportation permit and certification card may make an unlimited number of trips on a way in accordance with 700 CMR 7.07(6)(d) or a portion of a way as designated on the permit or certification card; the operator of the vehicle must carry an original, not a copy, of the certification card in an accessible place and must display it to a toll collector, other official or employee of the Department, or Massachusetts State Police officer on demand; and a vehicle for which the Department has issued such a permit must conspicuously display, both before and after, signs with letters not less than six inches in height bearing appropriate words identifying the cargo, and, if empty, the cargo last carried.

3. Fees. The applicant must pay the fee that is specified on the permit application and in 700 CMR 7.07(3): *Table 5*. The applicant must submit with its application full payment for the application fee and for all additional fees for the number of vehicles specified in the application. All these fees are in addition to any regular toll charge that the Department assesses in accordance with 700 CMR 7.03.

4. Minimum Separation of Vehicles. No vehicle used to carry a special fuel, however propelled and whether or not containing a special fuel, may operate within 1,000 feet longitudinally of another vehicle carrying a special fuel.

7.07: continued

5. No Stopping. No vehicle used to carry a special fuel, however propelled and whether or not containing a special fuel, may stop on a way, including a service or rest area, unless the movement of the vehicle is obstructed; it is disabled; or the operator of the vehicle is following the directions or requirements of a Massachusetts State Police officer, a sign, or governing federal regulations.

6. Conformance with Law. The equipment, cargo, operator, and operation of a vehicle operating under a special fuel transportation permit must conform with all federal and state laws and regulations governing the transportation of special fuels by a motor carrier.

7.08: Limitations on Large Tandem Units

(1) Scope. 700 CMR 7.08 applies exclusively to large tandem units.

(2) Use of Ways. Tandem units are not permitted in the Tunnels. No operator may operate a large tandem unit on any way other than the Turnpike. An operator may operate a large tandem unit on the Turnpike only if the Department has issued a large tandem unit permit pursuant to 700 CMR 7.07(2).

(3) Configuration and Length. A complete large tandem unit consists of a tractor, first semi-trailer, dolly, and second semi-trailer. The length of either semi-trailer may not be in excess of 48 feet, and the total length of the combination, including the dolly and load, may not exceed 120 feet, provided, however, that the overall length of loaded tandem trailer automobile haulers may not exceed 108 feet and may be increased to 109 feet by load overhang.

(4) Maximum Gross Weight. A large tandem unit must be registered for the gross weight that it carries and certified by the original manufacturer to carry this weight. The vehicle weight of a large tandem unit may not exceed 127,400 pounds. The maximum gross weight of the tractor and first semi-trailer may not exceed 71,000 pounds. The maximum gross weight of each unit of dolly and semi-trailer may not exceed 56,400 pounds.

The maximum gross weight that may be carried upon any combination of units is limited by the maximum gross weight that can be carried upon each unit and its axles. The maximum gross weight for the unit of tractor and first semi-trailer is governed by this formula: 35,000 pounds plus 1,000 pounds per foot between the center of the foremost axle of the tractor and the center of the rearmost axle of the first semi-trailer. The gross load on a unit may not exceed the sum of the allowable gross loads on the axles, which are as follows:

Maximum gross weight on any one axle	22,400 pounds
Tandem axles on one vehicle (under ten feet apart) (Axles measuring less than 46 inches between axle centers are considered as one axle.)	36,000 pounds

The limit of 127,400 pounds permitted under 700 CMR 7.08(4) requires a minimum axle spacing of 92 feet, measured betwee n the center of the foremost axle of the tractor and the center of the rearmost axle of the rearmost semi-trailer. If the axle spacing is less, the permissible gross weight is correspondingly reduced.

(5) Size and Weight Limitations Generally. The provisions of 700 CMR 7.00 with respect to size and weight that are not inconsistent with 700 CMR 7.08(4) are applicable to large tandem units unless specifically excluded under the terms of a large tandem unit permit.

(6) Approval of Vehicle or Equipment Used to Tow. The owner or lessee of a large tandem unit must file a description of the tractor, dollies, and any semi-trailer used to tow another semi-trailer with the Department on Forms MTT-3, MTT-4, and MTT-5, respectively. The owner or lessee must obtain the Department's approval of the vehicles before they are used under a large tandem unit permit. The Department may withdraw its authorization to use the vehicles at any time at its sole discretion.

7.08: continued

(7) Certification of Tractors. No operator may operate a large tandem unit unless the Department has certified that the tractor of the unit is appropriate for the purpose. Both the tractor manufacturer of each tractor used in a large tandem unit and the owner or lessee of the unit must certify to the Department prior to the approval of the tractor that it is capable of hauling the maximum permissible gross load to be transported by the owner or lessee at a speed not less than 20 m.p.h. over the Turnpike. (The maximum grade on the Turnpike is 7.50%, and the length of the longest such grade is approximately 1.75 miles.) If it is determined after the tractor is in use as part of a large tandem unit that the tractor cannot meet this requirement, the Department's approval may be withdrawn, and, in that event, the tractor may not be used as part of a large tandem unit on the Turnpike until the gross loads are reduced, the tractor is modified, or other corrective measures are taken. Upon a new certification by both the tractor manufacturer and the owner or lessee that corrective measures have been taken and the tractor is now capable of complying with the minimum speed requirement, the Department may reinstate its approval of the tractor.

(8) Certification of Trailers. No operator may operate a large tandem unit unless the Department has certified that the trailer of the unit is appropriate for the purpose. In order to comply with 700 CMR 7.08(13), all semi-trailers, except the rear trailer used in tandem operation, must have sufficient structural strength to permit the satisfactory attachment of the coupling device (pintle hook or its equivalent) at the rear of the trailer, and each coupling device must be capable of towing a trailer and a dolly. The permittee shall certify to the Department that every trailer certified for use in tandem service is adequate for this service and, in addition, the trailer manufacturer on new equipment must certify the adequacy of the trailer. If the trailer has been modified to include a pintle hook, the fabricator must certify the adequacy of the pintle hook assembly. Every coupling dev ice must incorporate a no-slack design such as air take-up, fitted pin and socket, mechanical wedging, or similar coupler designs, that eliminate fore and aft slack in the coupling of dollies to semi-trailers. The no-slack feature of the coupler must be in constant operation while the tandem trailer combination is operated on the Turnpike. The coupler used on each semi-trailer, in conformance with 700 CMR 7.08(8), must be specified by the permittee on Form MTT-4, giving semi-trailer descriptions and the vehicle identification number on the permittee's records (company number) and must be filed with the Department in conformance with 700 CMR 7.08(6).

(9) Brakes.

(a) Compliance with Federal Regulations. The brakes on a vehicle or dolly converter or combination of vehicles used in a large tandem unit must comply with federal regulations as published in 49 CFR Part 393, Subpart C, as revised and effective on the date of the vehicle's entry upon or use of the Turnpike.

(b) Compliance with State Law. A vehicle or dolly converter or combination of vehicles used in a large tandem unit must meet the requirements of the provisions of the M.G.L. c. 90.

(c) Braking Devices Required. The brake application line of every large tandem unit certified on or after June 1, 1968, must be equipped with suitable devices to accelerate application and release of the brakes of the towed vehicles. These devices must be so arranged that the brake application signal does not pass directly through more than one trailer, but is dead-ended at the rear of the trailer or, alternatively, at the dolly, and the application signal then is retransmitted to the dolly and the second trailer. The devices required for retransmission of the application signal must be closely connected to and supplied by air reservoirs that have their air supplied to them by the emergency line. In the event of rupture of the application line on the towed vehicle of a large tandem unit, the loss of brake application must be limited upstream of the loss to those vehicles between the rupture and the first retransmission device.

(d) Brakes on Steering Axle. A tractor used in a large tandem unit must have brakes on the steering axle.

(10) Axles. A tractor used in a large tandem unit with a gross weight of more than 110,000 pounds must be equipped with tandem rear axles, each of which must be engaged to bear its full share of the load on the roadway surface.

7.08: continued

(11) Emergency Equipment. Each tractor used in a large tandem unit must be equipped at a minimum as follows:

(a) Federal Regulations. Emergency equipment as required by 49 CFR Part 393, Subpart H.

(b) Fuses. At least one spare fuse or other overload protective device, if the devices used are not of a reset type, for each kind and size used.

(c) Chains. One set of tire chains for at least one driving wheel on each side between October 15th and May 1st.

(d) Fire Extinguishers. Fire extinguishers that have an aggregate rating of 20 BC.

(12) Vehicle Identification. The owner or lessee shall stencil the tractor weight on the left side of each tractor used in a large tandem unit. The Department issues an identification number that the owner or lessee shall also stencil on the left side of each tractor used in a large tandem unit. The Department also issues a certificate bearing the complete description of a particular tractor, including the maximum permissible gross load to be transported, and the operator shall suitably protect and carry this certificate in the cab of the tractor that it describes. A vehicle certified for less than 127,400 pounds may not exceed the weight indicated on the certificate. The Massachusetts State Police and Department personnel may examine the certificate and compare its description with the vehicle in which the certificate is carried. A discrepancy between the description on the certificate and the actual description of the vehicle may result in the withdrawal of the approval of the particular tractor or all of the vehicles and equipment of the owner or lessee. Compliance with the Provisions Governing the Operation of Tandem Trailer Combinations of the New York State Thruway Department requiring the issuance of an identification number, its stenciling on the tractor, and the issuance of a certificate describing the tractor is compliance with the similar requirements of 700 CMR 7.08.

(13) Tandem Assembly. In the assembly of large tandem units prior to their operation on the Turnpike, the operator shall ascertain the total gross weight of each trailer of the proposed combination. In the event that the gross weights of the trailers vary by more than 20%, the operator shall couple them for each trip according to their gross weight, that is, with the heaviest trailer coupled to the tractor.

(14) Dollies, Safety Chains, and Cables.

(a) Converter Dolly. Every converter dolly certified on or after June 1, 1968, used to convert a semi-trailer to a full trailer may have either single or tandem axles. The operator shall couple the dolly with one or more safety chains or cables to the frame, or to an extension of the frame, of the motor vehicle by which it is towed. Attachment of these chains or cables to the pintle hook or to any other device on the towing vehicle to which the tow bar is attached does not meet this requirement; provided, however, that a separate place of attachment independent of the pintle hook on a pintle hook forging or casting may be used to attach the safety chains or cables to the towing vehicle.

(b) Slack in Chains or Cable. Safety chains or cables may have no more slack than is necessary to permit proper turning.

(c) Strength of Chain or Cable. Each chain or cable and each means of attachment must have an ultimate strength at least equal to the gross weight of the vehicle being towed.

(d) Connection of Chain or Cable. Chains or cables must be connected to the towed and towing vehicles and to the tow bar in a manner that prevents the tow bar from dropping to the ground in the event that the bar fails or becomes disconnected.

(e) Chain or Cable on Converter Dolly with Hinged Tow Bar. Every converter dolly with a hinged tow bar must be equipped with two safety chains, or cables, or a bridle arrangement of a single chain or cable, attached to its frame or axle at two points as far apart as the configuration of the frame or axle permits. These chains or cables must be either two separate pieces, each equipped with a hook or other means for attachment to the towing vehicle, or a single piece leading along each side of the tow bar from the two points of attachment on the towed vehicle and arranged into a bridle with a single means of attachment to be connected to the towing vehicle. When a single length of cable is used, a thimble and twinbase cable clamps must be used to form the forward bridle eye. The hook or other means of attachment to the towing vehicle must be secured to the chain or cables in a fixed position.

7.08: continued

(f) Chain or Cable on Converter Dolly without Hinged Tow Bar. Converter dollies with solid tongues and without hinged tow bars or other swivels between the fifth wheel mounting and the attachment joint of the tongue eye or other hitch device may be equipped with either one or two safety chains or cables, provided that, if only one chain or cable is used, it must be in line with the center line of the trailer tongue. The point of attachment of these chains or cables to a solid tongue converter dolly is optional provided only that the attachment is to the rear of the attachment of the tongue eye or other hitch device.

(g) Points of Attachment. Where two safety chains or cables are used and attached to the towing vehicle at separate points, the points of attachment on the towing vehicle must be located equally distant from, and on opposite sides of, the center line of the towing vehicle. Where two chains or cables are attached to the same point on the towing vehicle, and where a bridle or a single chain or cable is used, the point of attachment must be on the center line of the towing vehicle.

(h) Compliance with Federal Regulations. Coupling devices and towing devices must comply with the federal regulations as stated in 49 CFR Part 393, Subpart F, on the date of the large tandem unit or one of its component's entry upon or use of the Turnpike.

(15) Indication That Trailers Form One Unit. When the distance between the rear of the one semi-trailer and the front of the following semi-trailer is ten feet or more, the dolly must be equipped with a device, or the trailers must be connected along the sides with suitable material, that will indicate to other traffic that the trailers are connected and are operating as one unit. The Department must approve the type of device or connection prior to its use on a large tandem unit.

(16) Lighting. Each trailer in a tandem trailer combination must be equipped at a minimum with electric lamps and reflectors mounted on the vehicle as follows:

(a) Amber Clearance Lamps. Two amber clearance lamps on the front, one at each side of the trailer.

(b) Rear Lamps. On the rear: one red tail lamp; one red or amber stop lamp; two red clearance lamps, one on each side; two red reflectors, one on each side.

(c) Side Lamps. On each side: one amber side-marker lamp located at or near the front; one red side-marker lamp located at or near the rear, one amber reflector, located at or near the front; one red reflector, located at or near the rear.

(d) On Dolly Converter. Each dolly converter, when towed singly by another vehicle, and not as a part of a full Trailer, must be equipped with a minimum of one stop lamp, one tail lamp, and two reflectors on the rear.

(17) Equipment Inspection. The operator of a large tandem unit is responsible for ensuring that all certified tandem trailer equipment is systematically inspected and maintained by a competent mechanic and kept in first class condition. Inspection and maintenance of the equipment must be in accordance with the requirements outlined in 49 CFR 396.

After all of the component vehicles in a large tandem unit are completely hooked up, and prior to the departure of the large tandem unit from the assembly area, the operator, or a mechanic, shall, in addition to the pre-trip equipment inspection and use requirements set forth in 49 CFR 392.7 and 49 CFR 392.8, inspect the large tandem unit and make certain tests on the vehicle, equipment, and hook-up to determine whether each item is in safe and proper operating condition.

The items to be inspected and tests to be made include, but are not to be limited to, the following:

-Federal equipment inspection.
-Inspection of brake line to dolly and trailers.
-Inspection of electric lines to dolly and trailers.
-Inspection of coupling devices.

7.08: continued

Following this inspection and prior to departure from the assembly area, the operator shall complete and execute a tandem trailer inspection report form provided by the Department. A new inspection report must be prepared each time the component parts of the tandem trailer unit are rearranged, or the operator is replaced, or upon re-entry to the Turnpike after any valid departure. The operator shall keep an original inspection report in an accessible place in the vehicle for which it was prepared, and this original inspection report must be presented to an official or employee of the Department, or a Massachusetts State Police officer on demand.

(18) Registration of Operators. Proposed operators of large tandem units must be registered with the Department prior to operating such equipment on the Turnpike. Completed applications for registration must provide all specified driving, safety, and physical examination records and be accompanied by an official abstract of the driving record of the individual for whom it is being submitted. An applicant for registration as an operator of a large tandem unit must demonstrate to the Department that the applicant has a minimum of five years of tractor trailer driving experience. The Department issues a special identification card to each registered operator of a large tandem unit, and each registered operator shall carry this card and display it upon request to a Massachusetts State Police officer or Department personnel. A registered operator may hold a large tandem unit permit for two companies at the same time, provided that each company has filed an application for this permit with the Department and that the Department has approved this permit. The special identification card is valid only for the operation of tractors owned or leased by the company by whom the operator is employed. The Department may decline to register an applicant or cancel a registration at any time should the Department determine that operational or safety considerations warrant its doing so. An operator's qualification for and possession of a valid special identification card of the New York State Thruway Department satisfies the requirements of 700 CMR 7.08.

(19) Speed Regulations. The operator of a large tandem unit shall strictly comply with the speed regulations for these units. In particular, an operator of a large tandem unit shall strictly observe the 55 m.p.h. speed limit as well as any lower posted speed limit.

(20) Distance Between Vehicles. The operator of a large tandem unit shall maintain a minimum distance of 500 feet, or approximately two delineator spaces, under normal conditions between a large tandem unit and a vehicle traveling in front of it in the same travel lane, except when passing occurs.

(21) Insurance. In order to comply with the Department's insurance requirements for large tandem units, the permittee must supply the Department with either a duplicate copy of its automobile liability insurance policy or a certificate of insurance evidencing automobile liability coverage. The policy or certificate of insurance must include the insurance requirements found in the large tandem unit permit application or other applicable form or document provided by the Department.

(22) Passing. A large tandem unit may pass another vehicle traveling in the same direction only if the speed differential between the large tandem unit and the vehicle that the large tandem unit is overtaking is adequate to allow the large tandem unit to complete the passing maneuver and return to the unit's driving lane within a distance of one mile.

(23) Reports and Observation. The owner or lessee shall, upon request, furnish to the Department all data and information pertaining to an individual trip by a large tandem unit or the overall large tandem unit operations of the owner or lessee on the Turnpike. The owner or lessee shall afford representatives of the Department the opportunity to observe the large tandem unit operations on the Turnpike by riding in the cab of the tractor or using other prescribed methods, all in accord with governmental regulations and insurance requirements.

(24) Payment of Fees and Tolls. An applicant must pay the fees that are specified in the permit application and in 700 CMR 7.07(3): *Table 5*, and the toll charge. The toll for a large tandem unit is the toll charge based on the classification of the vehicle under 700 CMR 7.03(1).

7.08: continued

(25) Emergency Service and Towing Vehicles. An emergency service or towing vehicle that an owner or lessee uses to maintain its large tandem units may be certified for operation on the Turnpike on Form MTT-1, provided that the owner or lessee certifies on Form MTT-1 that:

(a) The emergency service or towing vehicle is completely equipped with emergency lighting equipment.

(b) The use of the emergency service or towing vehicle will conform to the provisions of 700 CMR 7.00.

(26) Renewal of Permits. The Department may renew a large tandem unit permit monthly or annually upon the owner's or lessee's submission of Form MTT-2 requesting renewal. Form MTT-2 must be accompanied by a letter, on company stationery, signed by a duly authorized designee of the owner or lessee requesting recertification of the equipment to be continued in use in the operation of the large tandem unit, which has been certified previously pursuant to 700 CMR 7.08(8). The letter must be substantially similar to and include the information set forth in the sample letter that the Department supplies entitled "Sample Letter for Recertification of Tandem Equipment". According to the following schedule, the Department may subject an owner or lessee of a large tandem unit to a probationary period or to a period of suspension of operations based on the owner's or lessee's cumulative violations of motor vehicle laws or regulations or 700 CMR 7.00 that occur within a permit's annual renewal period:

(a) three violations - six month renewal
(b) six violations - three month renewal
(c) nine violations - one month renewal
(d) 12 violations - suspension of large tandem unit permit

(27) Limitations on Permits. The Department may, at its sole discretion, and, in whole or in part, revoke or temporarily suspend at will a large tandem unit permit. The Department's issuance of a large tandem permit creates no property interest, and the Department retains the right to amend or repeal, in the Department's sole discretion and the exercise of its police or other powers, the provisions of 700 CMR 7.08 pursuant to which large tandem unit permits are issued. The Department may temporarily suspend large tandem unit operations at any time and for any reason. Should the Department temporarily suspend operations of large tandem units, for example, because of inclement weather, reconstruction, or other adverse operating conditions, an operator of a large tandem unit shall comply with the instructions of the Department or the Massachusetts State Police immediately or as promptly as safe operating practices permit.

(28) Makeup-breakup Areas. Tandem trailer units may be assembled and disassembled only in special makeup-breakup areas that the Department designates for this purpose. No combination consisting of a tractor, first semi-trailer and dolly, with or without a second semi-trailer, may leave the Turnpike and pass on to a public highway or road within the Commonwealth of Massachusetts unless permitted by law. The owner or lessee of a vehicle entering or leaving a makeup-breakup area shall supervise the movement of the vehicle across traffic to minimize the possibility of accidents. The owner or lessee of a tandem trailer unit shall employ appropriate and adequate protection devices, such as flags, flares, or lights, to warn and stop traffic while the vehicles are maneuvering. The owner or lessee of a tandem trailer unit is solely responsible for its vehicles and equipment, as well as their contents, while the vehicles and equipment are in a makeup-breakup area. Large tandem units or components of them, except dollies, may not be parked in makeup-breakup areas for more than eight hours. The use of makeup-breakup areas is restricted to trailers of registered owners or lessors that exceed 28 feet. A tandem trailer unit left in a makeup-breakup areas must be disassembled while parked in tandem lots. A trailer parked in a makeup-breakup area containing hazardous materials must have its cargo's shipping papers available in an accessible place on the front of the trailer for inspection by the Department or a Massachusetts State Police officer.

(29) Penalties. Whoever violates any provision of 700 CMR 7.08 shall be punished by a fine not exceeding $500 for every such offense.

7.09: Traffic, Operation, and Safety

(1) Signs and Orders.

(a) Signs. The Department erects signs on ways to implement the provisions of 700 CMR 7.00, for purposes of trial use, or in the event of an emergency. A person may not disobey a sign unless a Massachusetts State Police officer directs otherwise. A person may not purposefully strike, move, deface, injure, obstruct, or interfere with a sign. A person may not, in any manner or by any means, erect or otherwise deploy any sign, signal, marking, or any other device that would be a sign if the Department deployed it, except with the approval, and at the direction, of the Department.

(b) Orders. A person may not fail to comply with any lawful order, signal, or direction by voice, hand, whistle, or Massachusetts State Police officer.

(2) Traffic Control Signal. The operator of a motor vehicle approaching a traffic control signal exhibiting one or more colored lights shall obey the commands of the lights in accordance with their signification as specified in 700 CMR 7.09(2): *Table 9*.

TABLE 9

Description of Light	Meaning
Green Light	Proceed.
Green Arrow	Proceed as directed by arrow.
Red Light	Stop or lane closed to traffic.
Red X	Lane closed to traffic.
Amber Light (in any other location)	Proceed only as directed by a Massachusetts State Police officer.
Flashing Light	Reduce speed and proceed with caution and in compliance with any supplemental directions.

(3) Parking.

(a) General Parking Prohibitions and Conditions. No operator may leave a parked vehicle on a way, including in parking areas of a service or rest area, except within those areas where a sign indicates that parking is allowed. Any such sign may impose time limits or other restrictions as the Department deems appropriate. Unless otherwise indicated, parking in service area parking lots where the Department allows parking is limited to two hours. The Department may, if it determines that emergency measures are appropriate, immediately and without notice prohibit parking in areas previously opened to parking.

(b) Over-weight or Over-size Vehicles. Parking of an over-weight vehicle or an over-size vehicle is permitted only in service area parking lots. Parking of such vehicles in parking areas reserved for tandem units is prohibited.

(4) Parking Specifically Prohibited. Without limiting the scope or effect of 700 CMR 7.09(3)(a), parking is specifically prohibited in areas constituting, or designated by signs as constituting, any of the areas listed in 700 CMR 7.09(4): *Table 10*.

7.09: continued

TABLE 10

Type of Area	Limitation of Description. If Any
(a) No Parking area - posted	Sign posted or curb painted yellow for restricted area.
(b) No Parking area - tow zone	-
(c) No Stopping or Standing area	-
(d) Crosswalk	-
(e) Sidewalk	-
(f) Reserved area	-
(g) Area reserved for HP or DV plate parking	-
(h) Handicapped Ramp	-
(i) Median	-
(j) Designated truck or bus parking area	If the vehicle is not a truck or bus.
(k) Designated car parking area	If the vehicle is not a private passenger motor vehicle or motorcycle.
(l) Designated tandem trailer parking area	If the trailer is not part of the tandem unit.
(m) Hydrant area	If any portion of the vehicle is located within ten feet of a fire hydrant.
(n) Designated fire lane	
(o) Breakdown lane	Except as such parking is permitted in accordance with 700 CMR 7.12(1) and 700 CMR 7.12(2).
(p) Over Posted Time Limit	If the time that the vehicle has been parking exceed the time limit indicated on an applicable sign.
(q) Inspection Sticker	If the vehicle does not have a properly displayed, current, valid inspection sticker.
(r) Idling in excess of five minutes	-
(s) Emergency vehicle access	-
(t) Double parking	-
(u) Weather emergency	If the vehicle is parked on a way when an applicable sign prohibits parking during an issued or declared weather emergency.
(v) Outside of marked spaces	-
(w) Street cleaning	If the vehicle is parked on the day and time indicated on an applicable sign for street cleaning.

(5) Negligent Operation or Loading.

(a) Negligent Operation. An operator may not operate a vehicle carelessly or negligently or in disregard of the rights or safety of others or without due caution and circumspection.

(b) Negligent Loading. An operator may not operate a vehicle that is constructed, equipped, or loaded so as to endanger unreasonably or to be likely to endanger unreasonably individuals or property.

(6) Speed.

(a) In General: Reasonable and Proper. An operator may not operate a vehicle at a rate of speed greater than that is reasonable and proper, having due regard for traffic, the condition of the roadway, and the safety of the public and property.

(b) In General: Not Driving so as to Endanger. An operator may not operate a vehicle at a speed or in a manner so as to endanger unreasonably or to be likely to endanger unreasonably persons or property.

7.09: continued

(c) Maximum and Minimum Speed Limits. An operator may not operate a vehicle at a rate of speed greater than that of the maximum speed limit indicated in 700 CMR 7.09(6): *Table 11* for the way. An operator may not operate a vehicle in excess of any lesser maximum speed limit for the way that the Department has posted on a sign on the way. An operator may not operate a vehicle at a rate of speed less than that of the minimum speed limit indicated in 700 CMR 7.09(6): *Table 11* for the way except while traveling in a creeper lane, acceleration lane, or deceleration lane; over a portion of a way where the Department has posted a lesser minimum speed limit on a sign; when the vehicle is incapable of operation at the minimum speed because of mechanical failure; when weather or roadway conditions require traveling at a lesser speed; or if the vehicle is an over-weight vehicle or over-size vehicle operating in conformance with a special permit, in which case the vehicle must be capable of maintaining a minimum speed of 20 miles per hour unless the special permit provides otherwise.

TABLE 11

Way	Maximum Speed Limit	Minimum Speed Limit
Turnpike between the New York State border and Interchange 14 in Weston, eastbound, and from Interchange 15 in Newton to the New York State border, westbound	65 m.p.h	40 m.p.h
Turnpike, all other portions	55 m.p.h	40 m.p.h
Callahan and Sumner Tunnels	35 m.p.h	20 m.p.h
Ted Williams Tunnel	40 m.p.h	20 m.p.h
Prudential Tunnel	45 m.p.h.	-
Thomas P. O'Neill, Jr., Tunnel	45 m.p.h.	-
Any Other Way	As posted.	As posted.
Entrance and Exit Ramps; entries and exits to toll plazas; and all other entries, exits, and ramps	As posted.	-

(7) Entering a Way. Except as otherwise directed by a Massachusetts State Police officer or sign, no individual may operate, push, or otherwise cause to move a vehicle on a way except in the direction of traffic. An operator of a motor vehicle entering a service or rest area, interchange, shoulder, or deceleration lane shall enter from the right hand travel lane. An operator of a motor vehicle entering a travel lane from a service or rest area or interchange shall use the acceleration lane and shall enter the travel lane with caution so as not to interfere with or endanger traffic.

(8) Travel Lanes. An operator may not drive a motor vehicle across solid pavement markings separating travel lanes unless a Massachusetts State Police officer, or sign so directs, or in the case of an emergency, or if done in accordance with 700 CMR 7.09(9).

(9) Breakdown Lane. An operator of a motor vehicle may not use a breakdown lane unless authorized by a Massachusetts State Police officer or a sign or the motor vehicle is a disabled vehicle.

(10) Crossing a Median or Area Not Intended for Travel.

(a) General Prohibition. An operator may not drive a motor vehicle upon or across a median or any area that has not been constructed or intended for travel except at the direction of a Massachusetts State Police officer or sign or in conformance with 700 CMR 7.09(10)(b).

7.09: continued

(b) Use of Cross-over. An operator may not drive a motor vehicle across a cross-over unless the motor vehicle is a Department vehicle or a vehicle that the Department has authorized in writing to be driven across a cross-over. Before such a vehicle uses a crossover, except one located at a Massachusetts State Police barracks or an Department maintenance depot, the operator shall drive onto the right shoulder and stop until the pavement can be crossed in safety. After the vehicle, except one plowing snow or sanding a way, has entered the cross-over, the operator shall again stop the vehicle until entry can be made on to a travel lane without presenting a hazard to through traffic. The operator of a vehicle plowing snow or sanding a way shall cause the vehicle to remain stopped on the right shoulder until both roadways on either side of the cross-over can be crossed in safety in a single movement without presenting a hazard to through traffic.

(11) Restricted Areas.

(a) In General. An operator may not drive a motor vehicle upon any portion of a way when, by reason of construction, surface treatment, maintenance, or the like, or because of some unprotected hazard, the portion of the way is closed to travel or use as indicated by a sign or by a Massachusetts State Police officer.

(b) Left Lane Restrictions on the Turnpike. On the Turnpike between Interchange 14 in Weston and Interchange 9 in Sturbridge, in both directions, no operator of a heavy commercial vehicle other than a bus may, except in an emergency, use any travel lane other than the extreme right-hand travel lane or, when overtaking and passing another vehicle, the next adjacent travel lane. East of Interchange 15 of the Turnpike in Weston, in both directions, no operator of a heavy commercial vehicle, bus, or vehicle with anything in tow may use any travel lane other than the extreme right-hand travel lane, or, when overtaking and passing another vehicle, the next adjacent travel lane, except in an emergency or when access to or egress from the turnpike is provided by the extreme left lane, and, in this circumstance, the operator shall use the extreme left lane only to the extent reasonably necessary to enter or leave the Turnpike safely.

(12) Construction Zones. The Department posts signs notifying operators that they are entering a construction zone or maintenance work zone on a way, indicating the speed limit within the zone, and indicating the fine for speeding within the zone as provided in 700 CMR 7.13(3)(a).

(a) Excess Speed. An operator may not drive a vehicle in such a zone at a speed in excess of the posted speed limit. In accordance with M.G.L. c. 90, § 17, any person operating a motor vehicle through the parameters of a marked construction zone or construction area, at a speed which exceeds the posted limit, or at a speed that is greater than is reasonable and proper, shall be subject to a fine of two times the amount currently in effect for the violation issued.

(b) Excluded Zone. An operator may not drive a vehicle in areas within such a zone from which the vehicle is excluded as indicated by a sign.

(c) Careless Manner or Purposeful Interference. An operator may not operate a vehicle in such a zone in a careless manner, including striking, moving, or interfering with a sign.

(13) Keeping to the Right.

(a) In the Tunnels. The operator of a truck, bus, school bus, or slow-moving motor vehicle in the Tunnels shall drive only in the right-hand lane unless a Massachusetts State Police officer, or sign otherwise directs.

(b) On Ways Other than the Tunnels. The operator of a motor vehicle on a way other than the Tunnels shall drive in the lane nearest the right shoulder of the roadway, when that lane is available for ordinary travel, except when overtaking another vehicle in that lane or at the direction of a Massachusetts State Police officer or sign. When the lane nearest the right shoulder of the roadway is a creeper lane or breakdown lane, an operator shall drive in the lane adjacent to the creeper lane or breakdown lane, except when overtaking another vehicle in that lane or at the direction of a Massachusetts State Police officer or a sign.

7.09: continued

(14) Passing. An operator of a motor vehicle may not overtake, attempt to pass, or pass another vehicle in violation of 700 CMR 7.09(8). An operator of a motor vehicle overtaking another vehicle shall, when necessary, signal that vehicle and also any vehicle to the rear in sufficient time before attempting to pass to give ample warning of such movement. If both the overtaking vehicle and the vehicle being overtaken are in the same lane, the operator of the overtaking vehicle shall gradually cross to an adjacent lane, which may not be a paved shoulder or a creeper lane, so as to avoid a sudden turn and to allow the overtaking vehicle to pass the overtaken vehicle at a safe lateral distance. The operator of a motor vehicle about to be overtaken and passed by another vehicle shall continue in the lane then occupied by the overtaken vehicle and may not increase the speed of the vehicle until it is completely passed by the overtaking vehicle. An operator of a motor vehicle may overtake, attempt to pass, or pass another vehicle in the same lane.

(15) Space Between Vehicles. The operator of a motor vehicle may not follow another vehicle more closely than is reasonable and prudent, having due regard for the speed of the vehicle and traffic conditions.

(16) Coasting. No operator may operate a motor vehicle without engaging the gears of the motor vehicle's transmission.

(17) Stopping, Backing, or Turning.

(a) Restrictions on Stopping, Standing, or Parking. The operator of a vehicle may not stop, stand, or park the vehicle except in conformance with 700 CMR 7.09(3) or (4); when necessary to avoid injury or damage to individuals or property; in compliance with the direction of a traffic control signal or sign; in compliance with the direction or signal of a Massachusetts State Police officer; or because the vehicle is a disabled vehicle that is repaired or removed in conformance with 700 CMR 7.12(1) or (2).

(b) Backing and U-turns Prohibited. Except as provided in 700 CMR 7.09(10), no operator of a motor vehicle may back the motor vehicle or make a U-turn on a travel lane, acceleration lane, breakdown lane, creeper lane or ramp.

(c) Care in Stopping or Turning. An operator, before stopping a vehicle or making any turning movement that would affect the operation of any other vehicle, must give a plainly visible signal by activating the brake lights or directional lights or signal as provided on the vehicle. In the event that electrical or mechanical signals are not operating or not provided on the vehicle, the operator must make a plainly visible signal by means of the left hand and arm as follows:

Intention to turn to the left:	Hand and arm extended horizontally.
Intention to turn to the right:	Hand and arm extended upward.
Intention to stop or decrease speed:	Hand and arm extended downward.

(18) Repairs and Removal of Disabled Vehicles. No person may repair or remove a disabled vehicle except in accordance with the applicable provisions of 700 CMR 7.12.

(19) Over-height Vehicles. The operator of a vehicle that activates a red light signal or the sounding of a buzzer warning that the vehicle is over-height shall immediately bring the vehicle to a stop and may not proceed further unless a special permit that the Department issues authorizes such travel.

(20) Cutouts. No operator of a motor vehicle may use any cutout or other apparatus or device that allows exhaust gas to escape into the atmosphere without passing through a muffler or silencer.

(21) Horn. No operator may sound a vehicle's horn or other device or in any manner operate the vehicle so as to make a harsh, objectionable, or unreasonable noise.

7.09: continued

(22) Headlights.

(a) In the Tunnels. No operator may flash the headlights of a motor vehicle or operate the motor vehicle with its headlights on high beam in the Tunnels, except on surface or aboveground roads or ramps of the Tunnels, provided that such use is warranted for reasons of safety.

(b) On Ways Other than the Tunnels. Whenever there is sufficient light within the traveled portion of a way other than the Tunnels to make clearly visible to the operator of a vehicle all other vehicles, individuals, or substantial objects for a distance of 350 feet, or whenever the operator of a vehicle approaches an on-coming vehicle within 500 feet, the operator shall regulate or operate the headlights of the vehicle so that no dangerous or dazzling light when measured 75 feet or more ahead of the headlights on a surface of uniform grade, rises to a height greater than 42 inches above the grade.

(23) Adequate Fuel. No operator of a motor vehicle may enter a way unless the motor vehicle carries a fuel or energy supply in its main fuel reservoir or energy supply source sufficient to enable it to complete its passage on the way without stopping to refuel or re-energize, except at designated service areas.

(24) Disposal of Waste or Other Materials.

(a) Minor Waste Disposal. No individual may dispose of household or commercial garbage or refuse other than by placing it in a trash barrel that the Department has placed on a way for the convenience of the traveling public.

(b) Major Waste Disposal. No individual may willfully place or drop on or from a way an article that may cause injury or death to an individual or damage to property, or improperly dispose of an article or waste material of any kind or description.

(25) Defacing. No person may cut, mutilate or remove a tree, shrub, or plant located on a way. No person may paint, mark, or mar any wall, bridge, or other structure on a way.

(26) Inspection Stickers. No vehicle may travel on a way unless it properly displays a current, valid inspection sticker pursuant to M.G.L. c. 90, § 7A, or the law of another jurisdiction in which the vehicle is registered as indicated by the number plate displayed by the vehicle.

(27) Inadequate Equipment. No operator may operate a vehicle in a manner that would violate any requirement as to the use of brakes, directional signals, lights, or safety devices and equipment specified in M.G.L. c. 90 with respect to the operation of a similar vehicle operating upon a way of the commonwealth.

(28) Idling. An operator of a motor vehicle shall comply with the provisions of M.G.L. c. 90, § 16A, regarding the unnecessary operation of the engine of a motor vehicle.

(29) Transportation of Alcoholic Beverages. No vehicle may travel on a way unless the operator complies with the provisions of M.G.L. c. 138, § 22, regarding the transportation of alcoholic beverages.

(30) Inspection and Examination of Cargo. No motor carrier may travel on a way unless it complies with the provisions of M.G.L. c. 159B, § 14A, with respect to the inspection and examination of cargo and of papers relating to cargo.

(31) Interstate Transportation. No vehicle may travel on a way unless it complies with the provisions of M.G.L. c. 159B, § 10, regarding interstate transportation.

(32) Operator's Record of Duty Status. An operator who 49 CFR 395 (1997) requires to keep a record of duty status must maintain and carry this record and present it to a Massachusetts State Police officer or other Department official upon demand.

7.10: Motor Carrier Safety Act

The Department hereby adopts and incorporates by reference into 700 CMR 7.00, with full force and effect and subject to other applicable provisions of 700 CMR 7.00, 49 CFR 325, 390-393, 395-396, and 399 (1997), governing highway safety and noise emissions. All operators shall conform to the requirements of these provisions.

7.11: Hazardous Materials

(1) In the Tunnels. Passenger or commercial vehicles carrying any amount of hazardous material, excluding those permissible materials required for the actual operation of the vehicle, may not enter or use the Tunnels. Hazardous material is defined and listed in 49 CFR Chapter 1, Subchapter C. Official emergency vehicles, as defined in 700 CMR 7.02 are exempt.

(2) On Ways Other than the Tunnels. The Department adopts the regulations set forth in 49 CFR Parts 171, 172, 173, 177, 178, and 179 and 10 CFR Part 71, subject to the exclusions set forth in 700 CMR 7.11(3), for the purpose of governing the transportation of hazardous materials upon a way other than the Tunnels. The Department adopts 49 CFR Parts 171, 172, 173, 177, 178, and 179 and 10 CFR Part 71 as fully applicable to the transportation of hazardous materials upon a way other than the tunnels and without their limitation to transportation in commerce. No person may offer, accept, or transport a hazardous material upon a way other than the Tunnels unless the material is properly classed, described, packaged, marked, labeled, handled, placarded, and in proper condition for shipment in accordance with 49 CFR and 10 CFR on the date of the hazardous material's entry upon a way other than the Tunnels.

(3) Inapplicable Federal Regulations. The Department does not adopt under 700 CMR 7.11(2) the following regulations set forth in 49 CFR Parts 171, 172, 173, 177, 178, or 179:

(a) Those regulations that apply to the transportation of hazardous materials by air, water, rail, or pipeline; and,

(b) Those regulations that require the reporting of hazardous material incidents, including, but not limited to, 49 CRR Parts 171.15 and 171.16.

(4) Exemptions. The persons and vehicles identified in 700 CMR 7.11(4)(a) and (b) are exempt from the requirements of 700 CMR 7.11(2):

(a) A person properly operating under a valid exemption under 49 CFR Part 107, subpart B is in compliance with those portions of 700 CMR 7.00 to which the exemption applies.

(b) The operator of a cargo tank vehicle engaged in the retail delivery of fuel oil is exempt from the shipping paper requirements set forth in 49 CFR Part 172, subpart C. The operator of a cargo tank vehicle engaged in the retail delivery of fuel oil shall comply with the placarding requirements set forth in 49 CFR Part 172.

(5) Construction and Priority of Application. 700 CMR 7.11(2) established the minimum standards with which an operator and vehicle transporting hazardous materials must comply. In the event of a conflict between 700 CMR 7.11(2) and another provision of 700 CMR 7.00, the more stringent standard applies.

(6) Application in an Unusual Situation. The Department may determine not to apply a provision of 700 CMR 7.11 to an individual set of circumstances if, after consideration of the facts involved, the Department determines that its application of the provision would not be in the public interest.

7.12: Repair or Removal of Vehicle

(1) In the Tunnels.

(a) Repairs. Repairs to a disabled vehicle in the Tunnels are prohibited unless authorized by the Chief Engineer or a Massachusetts State Police officer to ensure the safe and efficient operation of the Tunnels.

(b) Removal. The Department may immediately remove, or cause to be removed, a disabled vehicle or abandoned vehicle in the Tunnels, and the Department may park, garage, or store the removed vehicle on property of the Department or elsewhere, all at the risk and expense of the owner of the removed vehicle.

7.12: continued

(2) On a Way Other than the Tunnels. The provisions of 700 CMR 7.12(2) apply only to activities involving a disabled vehicle or abandoned vehicle that is located on a way other than the Tunnels. Activities involving a disabled or abandoned vehicle in the Tunnels are governed by 700 CMR 7.12(1).

(a) Repairs. The operator of a disabled vehicle may repair it, or cause it to be repaired in accordance with 700 CMR 7.12(2)(c), provided that the wheels and projecting parts, including any load, of the disabled vehicle completely clear the nearest lane by a minimum of two feet; the operator does not leave the disabled vehicle unattended; and the repairs are completed within two hours.

(b) Removal.

1. Authorization. The Department may remove, or cause to be removed, an abandoned vehicle in accordance with 700 CMR 7.12(2)(c). The Department may remove, or cause to be removed, a disabled vehicle in accordance with 700 CMR 7.12(2)(c) if effective repairs in accordance with 700 CMR 7.12(2)(a) cannot be accomplished or if, at any time, a Massachusetts State Police officer or the Chief Engineer determine that the vehicle's removal is appropriate to ensure the safe and efficient operation of the way.

2. Immediate Procedure. Pending removal in accordance with 700 CMR 7.12(2)(c), the operator of a disabled vehicle shall, if practicable, move or cause to be moved the vehicle to the extreme right side of the pavement or to an interchange. A Massachusetts State Police officer may similarly move a disabled vehicle or an abandoned vehicle.

(c) Providers of Repair or Removal Services.

1. Removal Procedure and Terms. A provider of emergency road services, as authorized in 700 CMR 7.12(2)(c), removes a disabled vehicle or an abandoned vehicle by towing, pushing, or transporting the vehicle at the risk and expense of its owner to a convenient place of storage as determined by a Massachusetts State Police officer or the Chief Engineer. The Department does not permit such a vehicle to be removed from the place of storage until full payment has been made for storage, towing, and any other charges reasonably related to the vehicle's removal.

2. Providers Certified with Respect to Tandem Units. The operator or owner of a tandem unit that is a disabled vehicle may use an emergency road-service provider certified in accordance with 700 CMR 7.08(25) to repair or remove the disabled vehicle; provided, however, that the Department or a Massachusetts State Police officer may require the tandem unit owner or operator to use a qualified towing contractor as described in 700 CMR 7.12(2)(c)3. to remove or repair the disabled vehicle if, in the judgment of the Department or the Massachusetts State Police, safety, the efficient operation of the way or the public convenience requires its doing so.

3. Qualified Towing Contractor. If the provisions of 700 CMR 7.12(2)(c)2. do not apply, a disabled vehicle or abandoned vehicle may be repaired or removed by a qualified towing contractor having a service contract with the Department and called to the scene by the Massachusetts State Police or the Department. Towing and related service charges are established in the service contract with the Department, and the qualified towing contractor provides a schedule of its charges to the vehicle owner or operator. The Department may terminate a service contract with a qualified towing contractor if the contractor fails to provide services in accord with its contract. Any person may submit written comments to the Chief Engineer concerning emergency road service that a qualified towing contractor provides.

4. Other Qualified Emergency Road-service Provider. At the request of the operator or owner of a disabled vehicle or abandoned vehicle, the vehicle may be repaired or removed by a qualified emergency road-service provider other than a qualified towing contractor as described in 700 CMR 7.12(2)(c)3.; provided, however, that the Department or a Massachusetts State Police officer may require the vehicle operator or owner to use a qualified towing contractor as described in 700 CMR 7.12(2)(c)3. to remove or repair the vehicle if, in the judgment of the Department or the Massachusetts State Police, safety, the efficient operation of the way or the public convenience requires its doing so.

7.13: Penalties

(1) Exemptions. 700 CMR 7.13 does not apply to, and the Department does not impose a penalty with respect to, an operator of a vehicle acting in conformity with the direction of a Massachusetts State Police officer, to the operator of a vehicle actually engaged in work on a way when the requirements of the work necessitate a departure from any of the requirements of 700 CMR 7.00 and the departure does not endanger the safety of individuals or property, or to a Massachusetts State Police officer when engaged in the performance of duties that necessitates a departure from any of the requirements of 700 CMR 7.00, or to the operator of an official emergency vehicle when an emergency necessitates departure from any of the requirements of 700 CMR 7.00. These exemptions do not, however, relieve such an operator from other legal consequences of the operator's or individual's action.

(2) *Prima Facie* Responsibility for Violations. If a vehicle is operated on a way in violation of any provision of 700 CMR 7.00 or any other regulation or law of the Commonwealth of Massachusetts, and the identity of the operator of the vehicle cannot be determined, the person in whose name the vehicle is registered is deemed *prima facie* responsible for the violation. With regard to a violation of 700 CMR 7.03(10), the person in whose name the vehicle is registered is deemed prima facie responsible for the violation, regardless of whether the operator of the vehicle may be identified.

(3) Fines.

(a) Fines by Reference to 700 CMR 7.00. Whoever violates any provision of 700 CMR 7.00 is subject to a fine not exceeding the amount indicated in 700 CMR 7.13(3): *Table 12*, in addition to other penalties as the laws of the Commonwealth of Massachusetts or federal law may provide. The section title and general subject matter headings are provided for convenience only and do not amend or in any way affect the substance of the provisions to which they refer.

TABLE 12

Section Title	Section	General Subject Matter	Fine Way other than the Tunnels	Fine Tunnels
Electronic Toll Collection	700 CMR 7.04(1)(a)	Unauthorized use of EZDRIVEMA System	Note 1	Note 1
	700 CMR 7.04(1)(b)	Restricted Access	Note 1	Note 1
	700 CMR 7.04(3)	Evasion of Toll	$250	$250
Limitation on Use of Ways	700 CMR 7.06(1)	Wrong way travel	$50	-
	700 CMR 7.06(2)	Wrong direction in Sumner, Callahan, or Ted Williams Tunnel	-	$500
	700 CMR 7.06(3)	Unauthorized entry or exit from a way	$50	$50
			-	$50

7.13: continued

Section Title	Section	General Subject Matter	Fine Way other than the Tunnels	Fine Tunnels
Prohibited Entry to or Use of a Way: Vehicle	700 CMR 7.06(4)(a)	Improperly seated person	$100	$100
	700 CMR 7.06(4)(b)	Flat or inadequate tire	$35	$35
	700 CMR 7.06(4)(c)	Obstructed window	$100	$100
	700 CMR 7.06(4)(d)	Muscle-powered vehicle	$100	$100
	700 CMR 7.06(4)(e)	Construction equipment	$100	$100
	700 CMR 7.06(4)(f)	Falling debris	$100	$100
	700 CMR 7.06(4)(g)	Inadequate brakes		
		1st Offense	$35	$35
		2nd Offense	$75	$75
		3rd and subsequent Offense within any 12 month period	$150	$150
	700 CMR 7.06(4)(h)	Over-weight vehicle	Note 2	Note 2
	700 CMR 7.06(4)(i)	Over-size vehicle	$500	$500
	700 CMR 7.06(4)(j)	Propelled by a special fuel	-	$500
	700 CMR 7.06(4)(k)	Carrying an explosive	$100	$100
	700 CMR 7.06(4)(l)	Carrying a special fuel	$500	$500
	700 CMR 7.06(4)(m)	Carrying a hazardous material	$500	$500
	700 CMR 7.06(4)(n)	Tandem unit, bulk liquid, radioactive materials, explosives, hazardous materials	-	$500
	700 CMR 7.06(4)(o)	Offensive odor, excessive smoke, improperly towed	$50	$50
Prohibited Entry to or Use of a Way: Non-vehicle	700 CMR 7.06(5)	Pedestrians and animals	$50	$50
	700 CMR 7.06(6)	Aircraft	$500	-
	700 CMR 7.06(7)	Hitchhiking or loitering	$50	$50
	700 CMR 7.06(8)	Commercial activity	$50	$50
Special Permits: General	700 CMR 7.07(2)(e)	Misrepresentation	$500	$500
	700 CMR 7.07(2)(f)	Invalid transfer	$500	$500
	700 CMR 7.07(2)(h)	Inappropriate use of Irreducible Load permit	$500	$500
	700 CMR 7.07(2)(j)	Inadequately insured vehicle operating under a Special Permit	$500	$500
	700 CMR 7.07(2)(m)	Operation of tandem unit in Tunnels - weight	-	$500
	700 CMR 7.07(3)(c)2.	Failure to carry original permit issued by the Department	$100	$100
	700 CMR 7.07(3)(c)3.	Failure to produce original Reducible Load (RL) Permit	$100/each permit	$100/each permit
	700 CMR 7.07(4)(c)2.	Failure to carry original permit issued by the Department	$100	$100
	700 CMR 7.07(4)(d)	Failure to conform with requirements for pilot car, police escort, or warning sign	$500	$500
	700 CMR 7.07(4)(e)	Prohibition on operation of Tandem unit and saddlemount combination (length) - Tunnels	-	$500
	700 CMR 7.07(4)(f)	Failure to exhibit height indication	$100	
	700 CMR 7.07(4)(g)	Insufficient care with respect to operation of over-size vehicle	$500	$100 $500

7.13: continued

Section Title	Section	General Subject Matter	Fine Way other than the Tunnels	Fine Tunnels
Special Permit: Vehicle Carrying an Explosive	700 CMR 7.07(5)(f)2.	Failure to carry original permit	$100	-
	700 CMR 7.07(5)(f)4.	Minimum separation	$500	-
	700 CMR 7.07(5)(f)5.	No stopping	$500	-
	700 CMR 7.07(5)(f)6.	Conformance with law	$500	-
Special Permit: Vehicle Carrying a Special Fuel	700 CMR 7.07(6)(e)2.	Failure to carry original permit	$100	-
	700 CMR 7.07(6)(e)2.	Failure to display signs	$100	-
	700 CMR 7.07(6)(e)4.	Minimum separation	$500	-
	700 CMR 7.07(6)(e)5.	No stopping	$500	-
	700 CMR 7.07(6)(e)6.	Conformance with law	$500	-
Limitations on Large Tandem Units	All provisions of 700 CMR 7.08		$500	-
Traffic, Operation, and Safety: General	700 CMR 7.09(1)(a)	Failure to obey sign	$50	$50
	700 CMR 7.09(1)(a)	Interfering with sign	$50	$50
	700 CMR 7.09(1)(a)	Deploying unauthorized sign	$50	$50
	700 CMR 7.09(1)(b)	Failure to comply with orders	$50	$50
	700 CMR 7.09(2)	Failure to obey traffic control signal	$50	$50
Traffic, Operation, and Safety: Parking Prohibitions	700 CMR 7.09(4)(a)	No parking area: posted	$50	-
	700 CMR 7.09(4)(b)	No parking area: tow zone	$50	-
	700 CMR 7.09(4)(c)	No stopping or standing	$50	-
	700 CMR 7.09(4)(d)	Crosswalk	$50	-
	700 CMR 7.09(4)(e)	Sidewalk	$50	-
	700 CMR 7.09(4)(f)	Reserved area	$50	-
	700 CMR 7.09(4)(g)	HP or DV plate parking only	$150	-
	700 CMR 7.09(4)(h)	Handicapped ramp	$100	-
	700 CMR 7.09(4)(i)	Median	$50	-
	700 CMR 7.09(4)(j)	Bus or truck parking area	$50	-
	700 CMR 7.09(4)(k)	Car parking area	$50	-
	700 CMR 7.09(4)(l)	Tandem trailer parking area	$50	-
	700 CMR 7.09(4)(m)	Hydrant	$50	-
	700 CMR 7.09(4)(n)	Designated fire lane	$100	-
	700 CMR 7.09(4)(o)	Breakdown lane	$50	-
	700 CMR 7.09(4)(p)	Over posted time limit	$50	-
	700 CMR 7.09(4)(q)	Inspection Sticker	$50	-
	700 CMR 7.09(4)(r)	Idling in excess of five minutes	$100	-
	700 CMR 7.09(4)(s)	Emergency vehicle access	$50	-
	700 CMR 7.09(4)(t)	Double parking	$50	-
	700 CMR 7.09(4)(u)	Weather emergency	$50	-
	700 CMR 7.09(4)(v)	Outside of marked spaces	$50	-
	700 CMR 7.09(4)(w)	Street cleaning	$40	

7.13: continued

Section Title	Section	General Subject Matter	Fine Way other than the Tunnels	Fine Tunnels
	700 CMR 7.09(5)(a)	Careless or negligent operation	$50	$500
	700 CMR 7.09(5)(b)	Negligent loading	$50	$100
	700 CMR 7.09(6)(a)	Reasonable and proper speed	$50	$50
	700 CMR 7.09(6)(b)	Operating at dangerous speed	$50	$500
	700 CMR 7.09(6)(c)	Maximum speed	Note 3	Note 3
	700 CMR 7.09(6)(c)	Minimum speed	$20	$20
	700 CMR 7.09(7)	Improper entry to a way	$50	$100
	700 CMR 7.09(8)	Crossing solid pavement markings	$50	$100
	700 CMR 7.09(9)	Unauthorized use of breakdown lane	$100	$100
	700 CMR 7.09(10)(a)	Unauthorized or dangerous crossing of median or other area	$50	$100
	700 CMR 7.09(10)(b)	Unauthorized use of cross-over	$50	$100
	700 CMR 7.09(11)(a)	Entry into restricted area - general	$100	$100
	700 CMR 7.09(11)(b)	Entry into restricted area - left lane restrictions	$100	$100
	700 CMR 7.09(12)(a)	Construction zone - excess speed (Note 5)	$100	$100
	700 CMR 7.09(12)(b)	Construction zone - entry into excluded area	$100	$100
	700 CMR 7.09(12)(c)	Construction zone - careless operation	$100	$100
	700 CMR 7.09(13)(a)	Keeping to the right when overtaking another vehicle - Tunnels	-	$100
	700 CMR 7.09(13)(b)	Keeping to the right when overtaking another vehicle - Non-tunnels	$100	-
Traffic, Operation, and Safety: Vehicle Operation	700 CMR 7.09(14)	Care in passing another vehicle	$100	$100
	700 CMR 7.09(15)	Space between vehicles	$100	$100
	700 CMR 7.09(16)	Coasting	$100	$100
	700 CMR 7.09(17)(a)	Stopping, standing, or parking	$50	$100
	700 CMR 7.09(17)(b)	Backing and U-turns prohibited	$50	$100
	700 CMR 7.09(17)(c)	Failure to use care in stopping or turning - hand signals	$25	$25
	700 CMR 7.09(18)	Repair or removal of disabled vehicle prohibited	$50	$50
	700 CMR 7.09(19)	Failure to respond to over-height alarm	-	$500
	700 CMR 7.09(20)	Improper use of cutouts	$35	$35
	700 CMR 7.09(21)	Improper use of horn	$35	$35
	700 CMR 7.09(22)(a)	Improper use of headlights - Tunnels	-	$50
	700 CMR 7.09(22)(b)	Improper use of headlights - Non-tunnels	$35	-
		Adequate fuel or energy supply		
	700 CMR 7.09(23)	Disposal of waste - minor	$50	$100
	700 CMR 7.09(24)(a)	Disposal of waste - major	$50	$50
	700 CMR 7.09(24)(b)	Defacing property	$100	$100
	700 CMR 7.09(25)	Failure to display inspection sticker	$500	$500
	700 CMR 7.09(26)	Inadequate equipment	$50	$50
	700 CMR 7.09(27)	1st Offense		
		2nd Offense	$35	$35
		3rd and subsequent Offense within any 12 month period	$75	$75
		Idling	$150	$150
	700 CMR 7.09(28)		Note 4	Note 4

7.13: continued

Section Title	Section	General Subject Matter	Fine Way other than the Tunnels	Fine Tunnels
Transportation of Cargo	700 CMR 7.09(29)	Transportation of alcoholic beverages	$100	$100
	700 CMR 7.09(30)	Inspection and examination of cargo	$100	$100
	700 CMR 7.09(31)	Interstate transportation	$100	$100
	700 CMR 7.09(32)	Operator's record of duty status	$50	$50
	700 CMR 7.10	Motor Carrier Safety Act	$50	$50
Hazardous Materials	700 CMR 7.11(1)	Hazardous Materials - Tunnels	-	$500
	700 CMR 7.11(2)	Hazardous Materials - Non-tunnels	$500	-
Repair and Removal of Vehicles	700 CMR 7.12(1)(a)	Unauthorized repair to disabled vehicle - Tunnels	-	$25
	700 CMR 7.12(1)(b)	Removal of disabled vehicle - Tunnels	-	$25
	700 CMR 7.12(2)(a)	Inappropriate repair of disabled vehicle - Non-tunnels	$25	-
	700 CMR 7.12(2)(b)	Removal of disabled vehicle - Non-tunnels	$25	-

Note 1: The fine for a violation of 700 CMR 7.04(1)(a) or 700 CMR 7.04(1)(b) or 700 CMR 7.03(10) is specified in 700 CMR 7.13(3)(b).

Note 2: The fine for exceeding the permissible weight is specified in 700 CMR 7.13(3)(c).

Note 3: The fine for exceeding the maximum speed limit is specified in 700 CMR 7.13(3)(d).

Note 4: The fine for idling is determined according to the provisions of M.G.L. c. 90, § 16A.

Note 5: The fine for speeding in a construction zone may be doubled in accordance with M.G.L. c. 90, § 17 and 700 CMR 7.09(12).

Note 6: The fine for a registered owner who fails to pay the fine specified in a violation notice or who fails to appeal a violation notice as provided by 700 CMR 7.14(1)(f) shall pay an additional penalty as indicated on the violation notice and/or in accordance with the amount in parenthesis in 700 CMR 7.07: *Table 11*.

(b) Fines for Failure to Pay Toll. The fine for a violation of 700 CMR 7.03(10) or 7.04(1)(a) or (b) is contained in 700 CMR 7.13: *Table 12*. Late payment fees may assessed in accordance 700 CMR 7.03(12) and 7.04(5).

(c) Fines for Over-weight Vehicles. Any operator who operates a vehicle, or any owner or bailee who requires or allows the operation of a vehicle, in violation of 700 CMR 7.06(5)(h) is subject to a fine of not less than $40.00 for each 1,000 pounds of weight or fraction thereof by which the vehicle weight of the vehicle as operated exceeds the maximum vehicle weight for a vehicle of its type as specified in 700 CMR 7.07(3): *Table 3*, or by a special permit that the Department issued for the vehicle for such operation, whichever is greater; provided, further, that, if the total of the excess weight is greater than 10,000 pounds, the rate of the fine is not less than $80.00 for each 1,000 pounds or fraction thereof over 10,000 pounds.

(d) Fines for Speeding. Any individual convicted of a violation of the maximum speed limit in violation of 700 CMR 7.09(6)(c) is subject to punishment by a fine of not less than $ 50.00. Where such conviction is for operating a motor vehicle at a rate of speed exceeding ten miles per hour over the speed limit, an additional fine of $10.00 for each mile per hour in excess of the ten miles per hour is assessed, to a maximum fine of $500.00.

(e) Fines for Other Violations. Whoever violates any provision of 700 CMR 7.00 not listed in 700 CMR 7.13(3): *Table 12* is subject to a fine not exceeding $500.00 for every such offense.

7.14: Parking Violation Enforcement

(1) Parking Violation Enforcement. The Department establishes regulations to address the public safety, environmental and related issues associated with the illegal parking of vehicles on properties owned, maintained or controlled by the Department.

(a) Enforcement. A violation or parking clerk may enforce the provisions of 700 CMR 7.14.

7.14: continued

(b) Designation of Violation Clerks. The Department may, from time to time, designate one or more violation or parking clerks to perform the functions specified in 700 CMR 7.14(1)(c) at the pleasure of the Department and for such finite or indefinite period as the Department deems desirable.

(c) Functions of the Violation Clerks. The State Police or a parking clerk designated by the Department will record and collect data to identify a violating vehicle and certify that such violation occurred. After the parking violation has been issued or affixed to the vehicle, copies of the parking violations are forwarded to the violation clerks for the processing of violation notices. The violation clerks may coordinate the processing of violation notices in accordance with 700 CMR 7.14(1). The Department may hire or designate such personnel and organize such divisions as the Department may deem necessary, or contract for such services, in order to carry out the provisions of 700 CMR 7.14.

(d) Content of Violation Notice.

1. Information Regarding the Specific Offense. A violation notice includes, but is not limited to, the following information: the registration number and state of issuance of the registration number of the vehicle involved; the make and color of the vehicle; the date, time and place of the violation; the specific violation charged by reference to the appropriate entry in 700 CMR 7.13(3): *Table 12*; the applicable fines or penalties that the Department has established; an identifier for the Department's designated representative who is certifying that the violation occurred; and instructions for the return of the tag; and such other information as the Department may deem appropriate.

2. Notice of Requirement to Respond. A parking violation notice states that the registered owner must pay the fine stated in the violation notice or appeal the violation within 60 calendar days after the date of the issuance of the violation notice and describes the means and content of the response for payment or appeal. Payments or appeals shall be received by the Department by the due date listed on the parking violation notice.

(e) Issuance of Violation Notice.

1. Delivery of Violation Notice. A parking violation notice shall be affixed securely to the motor vehicle. If it not possible to affix a parking violation notice to the motor vehicle, such notice shall be sent to the address of the registered owner of the motor vehicle, if the vehicle is registered in the Commonwealth of Massachusetts. If the motor vehicle is not registered in the Commonwealth, the parking violation notice shall be sent to the records of the official of the relevant state in charge of the registration of such motor vehicle.

2. *Prima Facie* Evidence of Notice. Notice affixed to a motor vehicle as provided in 700 CMR 7.14, shall be deemed a sufficient notice, and a certificate of the parking violation clerk affixing such notice that it has been affixed thereto, in accordance with 700 CMR 7.14, shall be deemed *prima facie* evidence thereof and the facts therein and shall be admissible in any judicial or administrative proceeding as to the facts contained therein.

(f) Payment or Appeal of Violation Notice. Within 60 calendar days after the date of the issuance of the parking violation notice, the registered owner to whom the violation notice is issued must make one of the following responses: pay the fine as provided by 700 CMR 7.14(f)1.; send a written dispute by mail as provided by 700 CMR 7.14(f)2.; or request a hearing as provided by 700 CMR 7.14(f)3.

1. Payment of Fine. The registered owner shall pay the fine as specified in the violation notice. Payment of the fine shall be received by the Department by the due date listed on the parking violation notice.

2. Appeal by Mail. The registered owner may, without waiving the right to a hearing before a violation clerk as provided by 700 CMR 7.14(f)3., and also without waiving judicial review as provided by M.G.L. c. 30A, § 14, appeal a parking violation and receive a review and disposition of the violation from a parking violation clerk by mail. The appeal by mail must contain a signed statement from the registered owner explaining the basis for the appeal. The signed statement may be accompanied by signed statements from witnesses, police officers, government officials, or other relevant parties or photographs, diagrams, maps or other relevant documents that the registered owner determines to submit. Statements or materials sent to a parking violation clerk for review must have attached to them the name and address of the registered owner as well as the number of the violation notice and the date of the violation. All information submitted

7.14: continued

by the registered owner becomes part of the violation record. Written appeals submitted by mail shall be received by the Department by the due date listed on the violation notice. The violation clerk shall, within 60 days of receipt of such material, review the material and dismiss or uphold the violation and notify the registered owner of the disposition of the hearing in writing by mail. If the appeal by mail is denied, the parking violation clerk shall explain the reasons for the determination. The review and disposition handled by mail is informal, the rules of evidence do not apply, and the decision of the violation clerk is final subject to the hearing provisions provided by 700 CMR 7.14(1)(f), and to judicial review as provided by M.G.L. c. 30A, § 14.

3. Request for Hearing. Consistent with the provisions of M.G.L. c. 30A, a person issued a violation notice may make a written request for an appeal hearing before a violation clerk designated by the Department. Requests for a hearing shall be received by the Department by the due date listed on the violation notice. The violation clerk then notifies the registered owner in writing by first class mail of the date, time, and place of the hearing. The hearing is informal, the rules of evidence do not apply, and the decision of the violation clerk is final, subject to judicial review as provided by M.G.L. c. 30A, § 14. Parties are notified in person or by mail of the decision following the hearing. Each written appeal decision contains a statement of reasons for the decision including a determination of each issue of fact necessary to the decision. Failure to appear at the date, time, and place specified on the hearing notice automatically results in the denial of the appeal.

(g) Failure to Comply. Failure to comply with the requirements of 700 CMR 7.14(1)(f) shall result in the following sanctions against the registered owner.

1. Additional Fines or Penalties. The Department may assess additional fines or penalties for late payment, failure to pay, or for otherwise failing to respond to a violation notice as provided by 700 CMR 7.14(1)(f).

Failure to Respond Within 60 Days after the Date of Issuance of a Violation Notice. A registered owner who fails to pay the fine specified in a violation notice or who fails to appeal a violation notice as provided by 700 CMR 7.14(1)(f) within 60 calendar days after the date of the issuance of the violation notice shall pay an additional penalty as indicated on the violation notice and/or 700 CMR 7.13(3): *Table 12*. The violation clerk notifies the registered owner by first class mail of this notice of liability and, in addition, notifies the Registrar of Motor Vehicles who shall place the matter on record and, upon receipt of a notice of liability, the Registrar shall not renew the registered owner's license to operate the vehicle or the registration of the vehicle until after notice from the violation clerk that all such matters have been disposed of in accordance with applicable law or regulation. If the registered owner is a resident of another state or jurisdiction, the Registrar shall revoke the registered owner's right to operate in the Commonwealth until the matter has been disposed of in accordance with applicable law or regulation.

2. Civil or Criminal Action. The Department may pursue such civil or criminal action as it deems appropriate to collect the fine initially assessed in the violation notice as well as such additional fines or penalties as the Department may assess in accordance with 700 CMR 7.14.

(2) Program Enforcement. Any violation notice based in whole or in part upon the written certification by the Department's designated representative for the purposes of recording such a violation, upon inspection of any photograph or other recorded image, and/or a violation clerk shall be *prima facie* evidence of the facts contained therein and shall be admissible in any administrative or judicial proceeding to adjudicate the liability for such violation. Nothing in 700 CMR 7.00 shall require a violation to be recorded by photographic or other recorded means, but a violation may be based in whole upon the written certification of the Department's designated representative that such violation has occurred.

7.14: continued

(3) *Prima Facie* Responsibility for Stolen Vehicle. The registered owner of any vehicle violating the provisions of 700 CMR 7.14 is *prima facie* responsible for the payment of the fines or penalties that the Department assesses in accordance with 700 CMR 7.13(3)(a) with respect to a violation of 700 CMR 7.14, unless the registered owner has reported in a timely manner to a police agency that the violating vehicle has been stolen, and the violating vehicle remained stolen at the time of the violation of 700 CMR 7.14.

REGULATORY DEPARTMENT

700 CMR 7.00: M.G.L. c. 6C, § 3(l).

Automated License Plate Readers

To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards for the Data It Collects

February 2020

REPORT 2019-118



CALIFORNIA STATE AUDITOR
621 Capitol Mall, Suite 1200 | Sacramento | CA | 95814

916.445.0255 | TTY **916.445.0033**

For complaints of state employee misconduct,
contact us through the **Whistleblower Hotline**:
1.800.952.5665

Don't want to miss any of our reports? Subscribe to our email list at **auditor.ca.gov**

For questions regarding the contents of this report, please contact Margarita Fernández, Chief of Public Affairs, *at* 916.445.0255

This report is also available online at www.auditor.ca.gov | Alternative format reports available upon request | Permission is granted to reproduce reports

Elaine M. Howle *State Auditor*

February 13, 2020
2019-118

The Governor of California
President pro Tempore of the Senate
Speaker of the Assembly
State Capitol
Sacramento, California 95814

Dear Governor and Legislative Leaders:

As directed by the Joint Legislative Audit Committee, my office conducted an audit of local law enforcement agencies' use of automated license plate readers (ALPR); the following report details the audit's findings and conclusions. In general, we determined that the law enforcement agencies we reviewed must better protect individuals' privacy through ensuring that their policies reflect state law. In addition, we found that these agencies must improve their ALPR data security, make more informed decisions about sharing their ALPR data, and expand their oversight of ALPR users.

We reviewed four agencies in detail that operate ALPR systems—Fresno Police Department, Los Angeles Police Department, Marin County Sheriff's Office, and Sacramento County Sheriff's Office. An ALPR system collects and stores license plate images of vehicles passing in its view and enables law enforcement to track a vehicle's movements over time; such a system raises privacy concerns. State law helps address these concerns by requiring agencies to have policies and safeguards in place to protect their ALPR systems from misuse. However, the agencies we reviewed either did not have ALPR policies or their policies were deficient, and they had not implemented sufficient safeguards. For example, none had audited searches of the ALPR images by their staff and thus had no assurance that the searches were appropriate. Furthermore, three of the four agencies have shared their ALPR images widely, without considering whether the entities receiving them have a right to and need for the images. The statewide survey of law enforcement agencies we conducted found that 70 percent operate or plan to operate an ALPR system, and this raises concerns that these agencies may share the deficiencies we identified at the four agencies we reviewed. Because many of the issues we identified link to the agencies' deficient ALPR policies we recommend that the Legislature direct the California Department of Justice to develop a policy template that local law enforcement agencies can use as a model for their ALPR policies.

Our statewide survey also showed that the period of time law enforcement agencies retain ALPR images varies widely. However, among the four agencies we reviewed none had considered the usefulness of the ALPR images to investigators over time when determining their retention periods. We recommend that the Legislature amend state law to specify a maximum retention period for ALPR images.

Respectfully submitted,

Elaine M. Howle

ELAINE M. HOWLE, CPA
California State Auditor

Selected Abbreviations Used in This Report

ACLU	American Civil Liberties Union
ALPR	Automated license plate reader
CHP	California Highway Patrol
CJIS	Criminal Justice Information Services Division
CLETS	California Law Enforcement Telecommunications System
FBI	Federal Bureau of Investigation
GPS	Global positioning system
ICE	U.S. Immigration and Customs Enforcement
IT	Information technology
OECD	Organization for Economic Cooperation and Development

Contents

Summary 1

Introduction 7

Audit Results
The Four Law Enforcement Agencies We Reviewed Have Not Consistently Fulfilled Requirements Designed to Protect Individuals' Privacy 15

The Law Enforcement Agencies Have Often Placed Their ALPR Data at Risk 18

The Law Enforcement Agencies Have Failed to Monitor Use of Their ALPR Systems and Have Few Safeguards for Creating ALPR User Accounts 32

Other Areas We Reviewed 39

Recommendations 40

Appendix A
Summary of ALPR Survey Responses 45

Appendix B
Scope and Methodology 49

Responses to the Audit
Department of Justice 53

Fresno Police Department 55

Los Angeles Police Department 59

California State Auditor's Comments on the Response From the Los Angeles Police Department 61

Marin County Sheriff's Office 63

California State Auditor's Comments on the Response From the Marin County Sheriff's Office 67

Sacramento County Department of Human Assistance 71

Sacramento County Sheriff's Office 73

California State Auditor's Comments on the Response From the Sacramento County Sheriff's Office 77

Blank page inserted for reproduction purposes only.

Summary

Results in Brief

To better protect the privacy of residents, local law enforcement agencies must improve their policies, procedures, and monitoring for the use and retention of license plate images and corresponding data. The majority of California law enforcement agencies (agencies) collect and use images captured by automated license plate reader (ALPR) cameras. The ALPR system is both a real-time tool for these agencies and an archive of historical images. Fixed cameras mounted to stationary objects, such as light poles, and mobile cameras mounted to law enforcement vehicles, capture ALPR images. Software extracts the license plate number from the image and stores it, with the date, time, and location of the scan and sometimes a partial image of the vehicle, in a searchable database. The software also automatically compares the plate number to stored lists of vehicles of interest, called *hot lists* then issues alerts, called *hits* if the plate number matches an entry on the hot list. Agencies compile these hot lists based on vehicles sought in crime investigations and vehicles connected to people of interest—for example, a list of stolen vehicles or of missing persons. We use the term *ALPR data* to describe all the information stored in an ALPR system, including license plate images and hot lists.

Because an ALPR system stores the plate number and image in a database even if the plate number does not match one on a hot list, the American Civil Liberties Union (ACLU) raised concerns in a 2013 report about law enforcement collecting and storing ALPR images related to individuals not suspected of crimes. The ACLU noted that law enforcement officers could inappropriately monitor the movements of individuals such as ex-spouses, neighbors, and other associates—actions that do not respect individuals' privacy. Although ALPR supporters contend that the images are collected in public places where there is no reasonable expectation of privacy, state law has made privacy a consideration when operating or using an ALPR system. Nonetheless, we found that the handling and retention of ALPR images and associated data did not always follow practices that adequately consider an individual's privacy.

Although law enforcement agencies collect ALPR images in public view, and there is no reasonable expectation of privacy regarding a license plate, the use and retention of those images raises privacy concerns. The four local law enforcement agencies we reviewed—Fresno Police Department (Fresno), Los Angeles Police Department (Los Angeles), Marin County Sheriff's Office (Marin), and Sacramento County Sheriff's Office (Sacramento)—have accumulated a large number of images in their ALPR systems, yet most of these images are unrelated to their criminal investigations.

Audit Highlights . . .

Our audit of the use of automated license plate readers (ALPR) at four local law enforcement agencies highlighted the following:

» *Local law enforcement agencies did not always follow practices that adequately consider the individual's privacy in handling and retaining the ALPR images and associated data.*

» *All four agencies have accumulated a large number of images in their ALPR systems, yet most of the images do not relate to their criminal investigations—99.9 percent of the 320 million images Los Angeles stores are for vehicles that were not on a* hot list *when the image was made.*

- *None of the agencies have an ALPR usage and privacy policy that implements all the legally mandated—since 2016—requirements.*
- *Three agencies did not completely or clearly specify who has system access, who has system oversight, or how to destroy ALPR data, and the remaining agency has not developed a policy at all.*
- *Two of the agencies add and store names, addresses, dates of birth, and criminal charges to their systems—some of these data may be categorized as criminal justice information and may originate from a system maintained and protected by the Department of Justice.*

continued on next page . . .

- *Three agencies use a cloud storage vendor to hold their many images and associated data, yet the agencies lack contract guarantees that the cloud vendor will appropriately protect the data.*
- *Three agencies share their images with hundreds of entities across the U.S. but could not provide evidence that they had determined whether those entities have a right or a need to access the images.*

» *Agencies may be retaining the images longer than necessary and thus increasing the risk to individuals' privacy.*

» *The agencies have few safeguards for creating ALPR user accounts and have not audited the use of their systems.*

For example, at Los Angeles only 400,000 of the 320 million images it has accumulated over several years and stores in its database generated an immediate match against its hot lists. In other words, 99.9 percent of the ALPR images Los Angeles stores are for vehicles that were not on a hot list at the time the image was made. Nevertheless, the stored images provide value beyond immediate hit alerts, as law enforcement personnel can search the accumulated images to determine the vehicles present at particular locations and to track vehicles' movements at particular times in order to gather or resolve leads in investigations.

Technology gives governments the ability to accumulate volumes of information about people, raising a reasonable question: How is an individual's privacy to be preserved? Effective in 2016 the California Legislature addressed privacy with respect to ALPR systems through Senate Bill 34 (Statutes of 2015, Chapter 532) (SB 34) by establishing requirements for these systems, including requiring detailed usage and privacy policies that describe the system's purpose, who may use it, how the agency will share data, how the agency will protect and monitor the system, and how long the agency will keep the data. Yet the agencies we reviewed have not implemented all of the requirements in that law.

Law enforcement agencies must first create policies that set clear guidelines for how they will use ALPR data. Setting certain expectations in writing through an ALPR usage and privacy policy helps ensure that agencies operate their ALPR programs in a manner that better protects individuals' privacy. However, none of the four agencies have an ALPR policy that contains all of the required information. In fact, Los Angeles has not developed an ALPR policy at all. The other three agencies did not completely or clearly specify who has system access, who has system oversight, or how to destroy ALPR data. Their poorly developed and incomplete policies contributed to the agencies' failure to implement ALPR programs that reflect the privacy principles in SB 34.

ALPR systems may contain data beyond license plate images. For example, we found that Sacramento and Los Angeles are adding names, addresses, dates of birth, and criminal charges to their ALPR systems, which are then stored in those systems. Some of these data may be categorized as criminal justice information; in addition, the data may originate from the California Law Enforcement Telecommunications System (CLETS), which the California Department of Justice (Justice) maintains. These various types of data require different levels of protection under the law. State law requires these agencies to maintain reasonable security procedures and practices to protect ALPR data from unauthorized access, destruction, use, modification, or disclosure. In addition, we believe that policy from the Criminal Justice Information Services

Division (CJIS) of the U.S. Federal Bureau of Investigation (FBI) models reasonable security measures for law enforcement agencies' ALPR data. CJIS policy specifies operational, administrative, technical, and physical safeguards for each of the areas specified in state law.

Fresno, Marin, and Sacramento use a cloud storage solution to hold their many ALPR images and associated data. Although the three agencies told us their systems comply with CJIS policy, none of them could demonstrate the vetting they performed to confirm that their cloud storage vendor did, in fact, meet the CJIS policy standards. Moreover, none of the contracts these three agencies have with their cloud storage vendors include all necessary data security safeguards. Thus, the agencies lack guarantees that the cloud vendor will provide appropriate protection of their data.

Law enforcement agencies of all types may benefit from guidance to improve their policies and data security practices. We surveyed 391 police and sheriff departments statewide, and of those using an ALPR system, 96 percent stated that they have ALPR policies, and nearly all reported that their ALPR data storage solution complies with CJIS policy. However, it is likely that many of the survey respondents have the same problems we identified at the four agencies we visited. Justice has experience guiding law enforcement agencies to help them adhere to state law and to improve their administrative practices. By developing guidance for local agencies on needed ALPR policy elements, Justice could help them improve the quality and completeness of their policies.

State law allows law enforcement agencies to share ALPR images only with public agencies, and it requires such sharing to be consistent with respect for individuals' privacy. Three of the reviewed agencies share their ALPR images widely using features in the ALPR systems that enable convenient sharing of images with minimal effort. Fresno and Marin have each arranged to share their ALPR images with hundreds of entities and Sacramento with over a thousand entities across the United States. However, we did not find evidence that the agencies had always determined whether an entity receiving shared images had a right and a need to access the images or even that the entity was a public agency. We are concerned that unless an agency conducts verifying research, it will not know who is actually using the ALPR images and for what purpose.

In addition, the agencies have not based their decisions regarding how long to retain their ALPR images on the documented usefulness of those images to investigators, and they may be retaining the images longer than necessary, increasing the risk to individuals' privacy. Fresno's policy is to retain ALPR images for

one year; Sacramento's and Marin's policies specify two years. Los Angeles does not have an ALPR policy, and the lieutenant who administers the ALPR program stated that its protocol is to retain the images for at least five years. However, when we reviewed the agencies' ALPR searches over a six-month period in 2019, we found that personnel for three of the four agencies typically searched for images zero to six months old. Nonetheless, the agencies keep the images far longer.

The agencies we reviewed have few safeguards for the creation of ALPR user accounts and have also failed to audit the use of their ALPR systems. Instead of ensuring that only authorized users access ALPR data for appropriate purposes, the agencies have left their systems open to abuse by neglecting to institute sufficient oversight. Over the years, the media has reported that some individuals within law enforcement used or could use data systems—and sometimes ALPR systems—to obtain information about individuals for their personal use, including to locate places they regularly visit, to determine their acquaintances, and to blackmail them based on this information. ALPR systems should be accessible only to employees who need the data, and accounts should be promptly disabled otherwise. However, the agencies often neglected to limit ALPR system access and have allowed accounts that should be disabled to remain active longer than is prudent. To further ensure that individuals with access do not misuse the ALPR systems, the agencies should be auditing the license plate searches that users perform, along with conducting other monitoring activities. Instead, the agencies have conducted little to no auditing and monitoring and thus have no assurance that misuse has not occurred.

Recommendations

Legislature

To better protect individuals' privacy and to help ensure that local law enforcement agencies structure their ALPR programs in a manner that supports accountability for proper database use, the Legislature should amend state law to do the following:

- Require Justice to draft and make available on its website a policy template that local law enforcement agencies can use as a model for their ALPR policies.

- Require Justice to develop and issue guidance to help local law enforcement agencies identify and evaluate the types of data they are currently storing in their ALPR systems. The guidance should include the necessary security requirements agencies should follow to protect the data in their ALPR systems.
- Establish a maximum data retention period for ALPR images.
- Specify how frequently ALPR system use must be audited and that the audits must include assessing user searches.

Law Enforcement Agencies

To address the shortcomings this audit identified, Fresno, Los Angeles, Marin, and Sacramento should do the following:

- Improve their ALPR policies.
- Implement needed ALPR data security.
- Update vendor contracts with necessary data safeguards.
- Ensure that sharing of ALPR images is done appropriately.
- Evaluate and reestablish data retention periods.
- Develop and implement procedures for granting and managing user accounts.
- Develop and implement ALPR system oversight.

Agency Comments

The four law enforcement agencies we reviewed responded to the draft audit report. Fresno responded that it will use the audit to work to achieve its goal of building trust in its community. Los Angeles responded that it respects individuals' privacy and believes it has policies in place to safeguard information. Nonetheless, it is working on an ALPR policy as required by state law and will perform periodic audits of users' searches. Marin stated it is committed to improvement and will consider the recommendations we made, although it disagreed with several of them. Sacramento stated that it had already begun implementing many of the recommendations, but that it did not agree with how we characterized some of the findings. Justice and the Sacramento County Department of Human Assistance also responded by acknowledging the draft report, although we did not have recommendations directed to either entity.

Blank page inserted for reproduction purposes only.

Introduction

Background

An automated license plate reader (ALPR) is a camera that captures color images of license plates within its field of view. Fixed cameras are mounted on stationary objects, such as light poles, while mobile cameras are mounted on moving objects, such as patrol cars. Software extracts the license plate numbers from the images and stores the images, plate numbers, and dates, times, and locations of the image captures in a searchable database. An *ALPR* system consists of the cameras, the software that reads and converts images of license plates into data, and the searchable database that stores the data. Although the primary focus of each image is the license plate, the image may also show part of the vehicle itself, including individuals within the vehicle, depending on the camera's position. ALPR technology has existed since the 1970s, yet widespread adoption by U.S. law enforcement agencies began only in the mid-2000s. Law enforcement agencies generally view ALPR technology as a valuable tool in achieving their missions.

We conducted a statewide survey of 391 police and sheriff departments, and the survey confirmed that ALPR use is widespread in California: 230 police and sheriff departments currently use an ALPR system, and 36 plan to use one. Table 1 provides an overview of the ALPR systems of the four law enforcement agencies we reviewed as part of this audit.

Table 1
ALPR Systems of Four Audited Law Enforcement Agencies

		NUMBER OF CAMERA SYSTEMS			
LAW ENFORCEMENT AGENCY	NUMBER OF AGENCY PERSONNEL WITH ACCESS TO ALPR DATA	FIXED	MOBILE	CURRENT ALPR VENDOR	DATE AGENCY BEGAN USING CURRENT ALPR VENDOR
Fresno	231	0	8	Vigilant Solutions, LLC	2016
Los Angeles	13,000	3	393	PIPS Technology*	2007
Marin	38	0	3	Vigilant Solutions, LLC	2010
Sacramento	539	33	27	Vigilant Solutions, LLC	2012

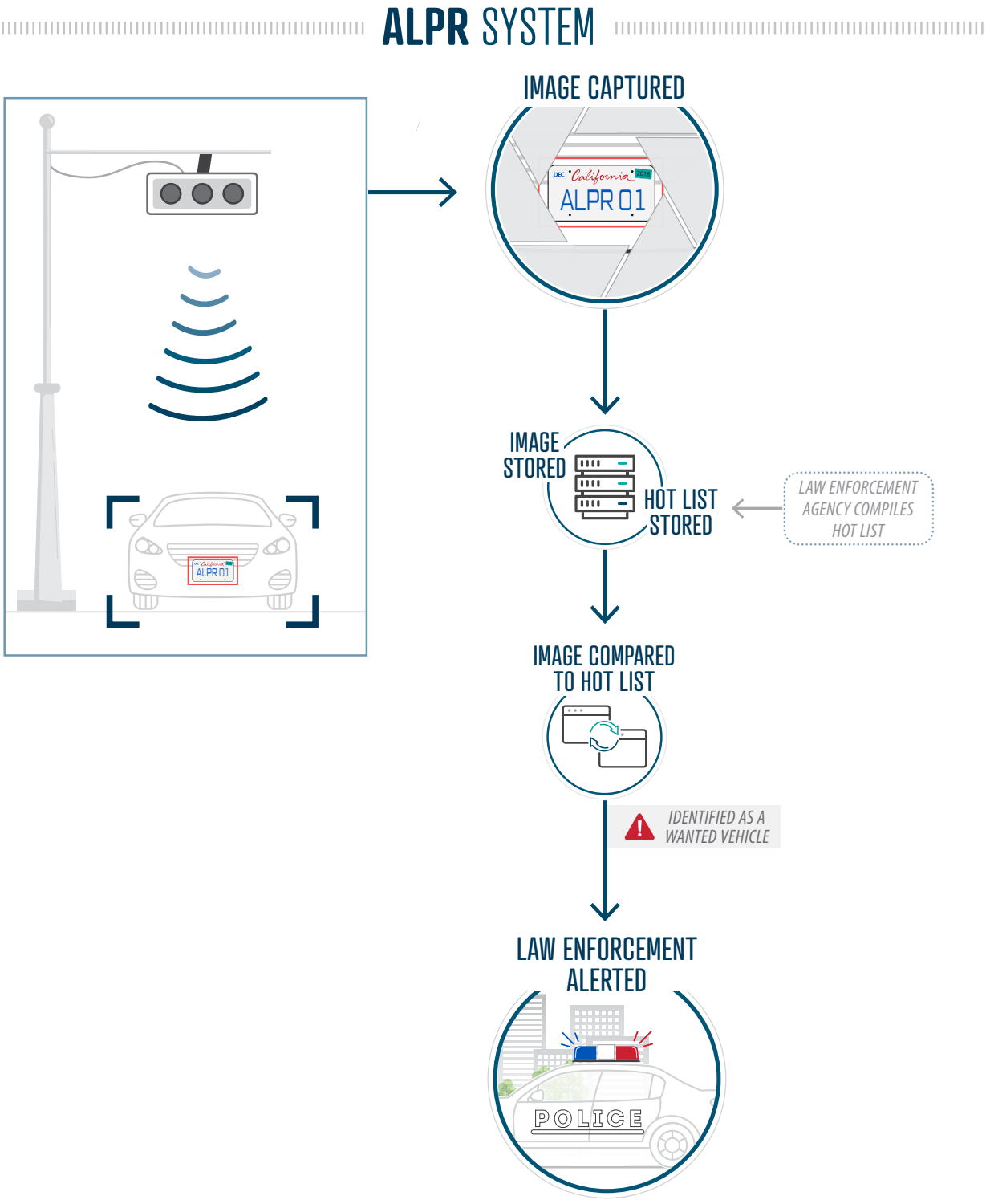
Source: Analysis of reports on ALPR systems as of 2019 and the agencies' survey responses.

* Los Angeles uses PIPS Technology cameras and a user interface from Palantir Technologies, Inc.

An ALPR system is both a real-time tool for law enforcement agencies and an archive of historical information. After the ALPR system identifies a license plate number in an image, it compares the plate number to stored lists of license plate numbers from vehicles of interest, called *hot lists*. Figure 1 shows how an ALPR system uses hot lists to search stored images. Local law enforcement agencies create their own hot lists and also obtain hot lists from state and federal agencies. For example, the California Department of Justice (Justice) provides hot lists to local agencies that include license plate numbers associated with missing persons, gang members, and suspected terrorists. We use the term *ALPR data* to describe all the information stored in an ALPR system, including license plate images and hot lists. Regardless of whether a license plate number matches a plate on a hot list (a *hit*), an ALPR system stores the plate image in a database, creating a searchable archive. Officers may search the database in various ways. For example, they may search for a full license plate number to locate a specific vehicle, search for a partial license plate number to locate a group of vehicles, or search for all vehicles recorded at a particular location at specific times.

Law enforcement agencies can share ALPR data with other public agencies. In the ALPR systems we observed, the agency could choose to share ALPR images only, to share hot lists only, or to share both. Accessing ALPR images shared from other jurisdictions enables agencies to search a broader area, such as across county and state lines. In addition, even if an agency does not operate ALPR cameras itself, it can, through sharing agreements, access ALPR images other agencies collect. Our statewide survey showed that among agencies that operate ALPR systems, roughly 84 percent share their images. Sharing hot lists also enables broader search coverage. For example, an agency could share a hot list that provides license plates linked to wanted individuals with other entities in the region. These entities would then receive hit alerts if their cameras detected those plates.

Figure 1
How ALPR Systems Work



Source: Analysis of David J. Roberts and Meghann Casanova, *Automated License Plate Recognition Systems: Policy and Operational Guidance for Law Enforcement*, International Association of Chiefs of Police, Washington, D.C., 2012.

ALPR Vendors Most Commonly Used in California

Law enforcement agencies typically contract with a third-party vendor for an ALPR system. In our statewide survey, most—70 percent—of those that have an ALPR system reported using a company called Vigilant Solutions, LLC (Vigilant). Figure A.1 in Appendix A summarizes these responses. Three of the agencies we reviewed—the Fresno Police Department (Fresno), Marin County Sheriff's Office (Marin), and Sacramento County Sheriff's Office (Sacramento)—contract with Vigilant. The Vigilant ALPR system provides a user interface to search license plates and the option to share ALPR images and hot lists with other agencies through the Vigilant system. Fresno, Marin, and Sacramento all store their ALPR images on Vigilant's server, which is a cloud service, and share their images with other agencies that subscribe to Vigilant's services. Roughly 22 percent of the survey respondents that have ALPR systems use a company called PIPS Technology. One of the agencies we audited in depth, the Los Angeles Police Department (Los Angeles), purchased its cameras from PIPS Technology, but it stores the images on its own server. Los Angeles uses a software platform called Palantir for the user interface that allows for searches of its ALPR images, and it shares its ALPR images with other agencies in the region that use the Palantir user interface.

Key Elements Law Enforcement Agencies Must Include in Their ALPR Usage and Privacy Policy

- The authorized purpose for using the ALPR system and collecting, accessing, or using ALPR data.
- A description of the job title or other designation of the employees and independent contractors who are authorized to use or access the ALPR system, or to collect ALPR data.
- The training requirements for those employees and independent contractors authorized to use or access the ALPR system, or to collect ALPR data.
- A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.
- The purposes of, process for, and restrictions on the sale, sharing, or transfer of ALPR data.
- The length of time ALPR data will be retained, and the process for determining if and when to destroy retained ALPR data.

Source: Analysis of state law.

State Laws Governing ALPR Systems and Data Sharing

With few exceptions, California law requires public agencies that operate and use ALPR systems to implement a usage and privacy policy. The Legislature passed Senate Bill 34 (Statutes of 2015, Chapter 532) (SB 34), effective January 1, 2016, to establish requirements regarding the operation and use of ALPR systems. This law generally requires public agencies, including law enforcement agencies, that operate or use an ALPR system to maintain reasonable security procedures and practices to protect ALPR data, to implement a usage and privacy policy, to make that policy available to the public, and to post that policy on its website should the agency have one, among other provisions. The text box describes required elements of an agency's ALPR usage and privacy policy.

SB 34 does not specify retention periods for ALPR data, although another state law limits the California Highway Patrol (CHP) to retaining its ALPR images for no more than 60 days, unless those images are being used for felony investigations or as evidence. Agencies implementing ALPR programs after January 1, 2016, must also provide an opportunity for public comment before implementing the program.

In 2018 another state law took effect that limits the information law enforcement agencies can share for immigration enforcement purposes and requires Justice to issue guidance to state and local law enforcement agencies regarding these limitations as they apply to law enforcement databases. In October 2018 Justice issued this guidance, which can also serve as best practices for law enforcement agencies on how to lawfully share ALPR images. The guidance encourages law enforcement agencies that maintain databases to inquire about the purpose for which the other law enforcement agency intends to use the information contained in the database. If a law enforcement agency intends to use the information for immigration enforcement purposes, Justice states that law enforcement agencies should require, as a condition of accessing the database, an agreement that stipulates that access will be made only in cases involving individuals with criminal histories, or for information regarding the immigration or citizenship status of an individual. Beyond this guidance and the hot lists Justice provides to local law enforcement agencies, as we describe earlier, Justice plays no other role in ALPR programs.

State law requires law enforcement agencies to maintain reasonable security procedures and practices to protect ALPR data from unauthorized access, destruction, use, modification, or disclosure. These requirements mean that ALPR data are sensitive. For comparison purposes, the California Department of Technology Office of Information Security defines *sensitive data* for state agencies as information that requires special precautions to protect it from unauthorized use, access, disclosure, modification, loss, or deletion. In addition to ALPR images and hot lists, a law enforcement agency can enter other information into its ALPR system, such as personal information and criminal justice information. *Personal information* is information that identifies or describes an individual, including name or physical description. SB 34—whose purpose was, in part, to institute reasonable privacy standards for the operation of ALPR systems—requires that ALPR data be protected with reasonable operational, administrative, technical, and physical safeguards to ensure their confidentiality. Thus, personal information in an ALPR system also requires appropriate and reasonable safeguards. *Criminal justice information*, as defined by the Criminal Justice Information Services Division (CJIS) of the U.S. Federal Bureau of Investigation (FBI), refers to data necessary

for law enforcement and civil agencies to perform their missions. This includes information about vehicles associated with crimes, when accompanied by personal information.

When CJIS provides criminal justice information to law enforcement agencies, it requires those agencies to comply with a minimum set of information technology (IT) security requirements to protect the information, and these requirements can serve as best practices for agencies to follow. Because an agency can enter personal information and criminal justice information into its ALPR system, either as part of a hot list or as a comment added as part of a license plate search, all ALPR data are sensitive and require appropriate safeguards.

Privacy Concerns Related to ALPR Systems

Although law enforcement agencies collect ALPR images in public view, and there is no reasonable expectation of privacy regarding a license plate, the use and retention of those images raises privacy concerns. The agencies we reviewed accumulate a large number of images in their ALPR systems. For example, Sacramento recorded 1.7 million images in one week, and Los Angeles currently has more than 320 million images in its ALPR database that it has accumulated over several years. The majority of these images do not generate hit alerts. For example, data from the Los Angeles system show that at the time of our review only 400,000 (0.1 percent) of the 320 million images Los Angeles has stored generated an immediate match against its hot lists for vehicles associated with car thefts, felonies, or warrants. However, the stored images provide value beyond immediate hit alerts, as law enforcement personnel can search the accumulated images to target the whereabouts of vehicles at particular times or locations. This storage, retention, and searching of the images, although valuable to law enforcement, has the potential to infringe on individuals' privacy.

Organizations such as the American Civil Liberties Union (ACLU) have criticized law enforcement agencies' collection of ALPR images because of the risks it poses to privacy. The ACLU stated that increasing numbers of cameras, long data retention periods, and sharing of ALPR images among law enforcement agencies allow agencies to track individuals' movements in detail, and it has voiced concerns that such constant monitoring can inhibit the exercise of free speech and association. The ACLU has also raised concerns that law enforcement officers could inappropriately monitor the movements of individuals such as ex-spouses, neighbors, and other associates. There have been occurrences of officers misusing law enforcement databases like those that contain ALPR images. In 2016 the Associated Press conducted a review that found more than

325 instances between 2013 and 2015 in which law enforcement officers who misused databases were fired, suspended, or resigned, and more than 250 instances of reprimands or lesser discipline related to such misuse. For example, the Associated Press reported on a police sergeant in Ohio who pleaded guilty to stalking his ex-girlfriend after he searched law enforcement databases for personal information about her and also the woman's mother, her close male friends, and students from a course she taught.

Law enforcement has recognized the privacy concerns posed by the operation of ALPR systems, yet it has also pointed to the usefulness of the systems. For example, the Police Executive Research Forum (police research forum) and the Mesa Police Department (Mesa) in Arizona conducted a study of the effectiveness of ALPR systems for Mesa's auto theft unit in 2011. They found that officers got nearly three times as many stolen vehicle hits and made about twice as many vehicle recoveries when using an ALPR system, compared to officers performing manual license plate checks. Law enforcement has also found ALPR systems useful for investigations. For example, the assistant chief of the Minneapolis Police Department told the police research forum in 2012 that the department located a vehicle associated with a domestic kidnapping case by searching ALPR images. With regard to the retention of ALPR images, the International Association of Chiefs of Police (chiefs' association) acknowledged the tension between long retention periods and privacy. The chiefs' association noted that a reluctance to destroy records may stem from investigators' experience that seemingly irrelevant or untimely information may acquire new significance as an investigation brings further details to light. However, the chiefs' association also recognized the privacy risks of ALPR images. In a 2009 report, it stated that mobile ALPR cameras could record license plate numbers of vehicles parked at addiction counseling meetings, doctors' offices, and staging areas for political protests. The chiefs' association argued that establishing policies regulating ALPR programs could mitigate privacy concerns, and it produced a report in 2012 offering guidance on developing such policies.

Federal Guidance on Privacy Protection

As far back as 1973, the federal government acknowledged that individuals' privacy needs to be protected from arbitrary and abusive record-keeping practices. The U.S. Department of Health, Education, and Welfare, as it was then known, identified principles for the fair collection, use, storage, and dissemination of personal information by electronic information systems. Over time the principles were adapted into information practices. According to the U.S. Government Accountability Office, a revised version of the information practices was published in 1980 by

the Organization for Economic Cooperation and Development (OECD)—an international organization that works with governments, policymakers, and citizens on social, economic, and environmental challenges—and with some variation, these practices form the basis of privacy laws in the United States and around the world. The OECD updated its eight information practices in 2013, and California's lawmakers included many of these information practices in SB 34. For example, the OECD's information practices describe the importance of an organization specifying the purposes for which it is collecting and using data; keeping data reasonably safe from the risk of unauthorized access, destruction, use, modification, and disclosure; being open about policies involving data; and being accountable for complying with the information practices.

The U.S. Supreme Court (court) has not directly decided a case that we could find addressing ALPR images, although it has decided cases involving other electronic surveillance. Because license plates are in plain view, the collection of license plate images by law enforcement is not a per se violation of the Fourth Amendment's prohibition against unreasonable searches and seizures. However, the court has found that certain electronic data that reveal individuals' movements over an extended period of time, if gathered, do at some point impinge on privacy. The court has specifically addressed these issues with respect to the use of global positioning system (GPS) data and cell-site location information, which is location information linked to cellphone use. Cell-site location information—similar to ALPR images—provides data on an individual's continuous movements over a potentially unlimited period of time. In a 2018 case involving cell-site location information, the court stated that "[a] person does not surrender all [privacy] protections by venturing into the public sphere." The court continued, "With access to [cell-site location information], the Government can now travel back in time to retrace a person's whereabouts," and noted that the information was collected on everyone, not only "persons who might happen to come under investigation." Thus, even though case law on electronic data that enable tracking of individuals' movements over an extended period of time is still evolving, the court has recognized that privacy implications exist for such data, which can include ALPR images.

Audit Results

The Four Law Enforcement Agencies We Reviewed Have Not Consistently Fulfilled Requirements Designed to Protect Individuals' Privacy

California's lawmakers drafted current ALPR law to institute reasonable privacy standards for the operation of ALPR systems. As we discuss in the Introduction, technology gives governments the ability to accumulate significant amounts of information about people, raising the question of how individuals' privacy is to be preserved, and the federal and state governments and courts have issued laws and guidance—including, in the case of California, SB 34—related to the use of such information.

Yet local law enforcement agencies—specifically the four agencies we reviewed—have not done all they could to respect individuals' privacy by incorporating the requirements and concepts in SB 34 into their operations. With few exceptions, SB 34 requires a public agency that operates or uses an ALPR system to implement a usage and privacy policy that describes how the system will be used and monitored to ensure the security of the ALPR data accessed or used. The agencies we reviewed have mature ALPR programs—they have been using their current ALPR vendors since as far back as 2007. However, as we discuss later, we found that the agencies have risked individuals' privacy by not making informed decisions about sharing ALPR images with other entities, by not considering how they are using ALPR data when determining how long to keep it, by following poor practices for granting their staff access to the ALPR systems, and by failing to audit system use.

State law requires law enforcement agencies to administer ALPR programs in ways that respect individual's privacy and protect ALPR data. The law also requires the agencies to have a written usage and privacy policy that sets forth how they will operate and use their ALPR systems. These usage and privacy policies must include the following elements:

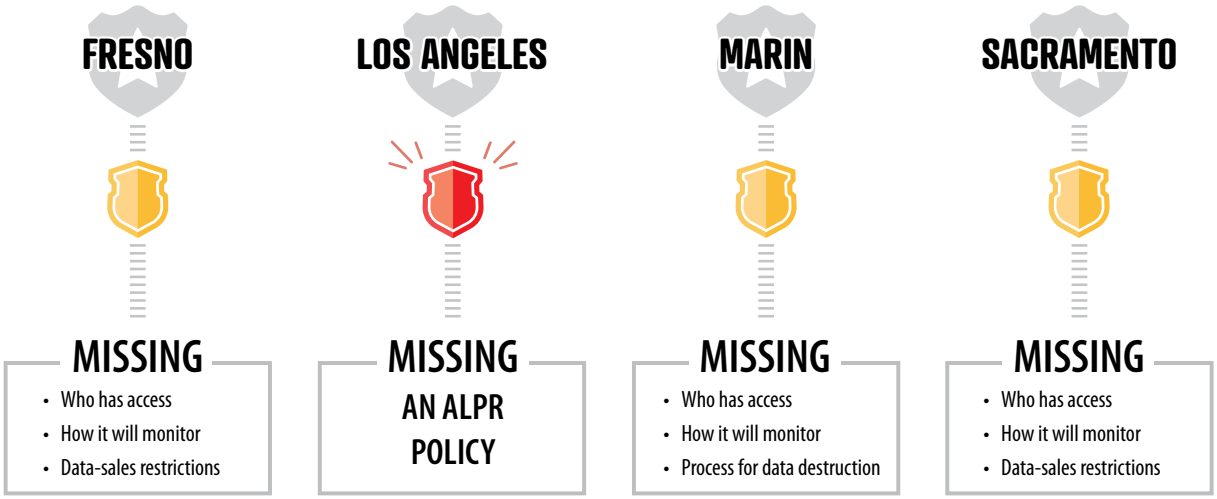
- Authorized purposes for using the ALPR system and collecting the data.
- A description of the job title or other designation of individuals who are authorized to use or access the ALPR system.
- Training requirements for the authorized individuals who will use or access the ALPR system.
- A description of how the agency will monitor the ALPR system to ensure the security of the data and compliance with privacy laws.

- The purpose of, process for, and restrictions on the sale, sharing, or transfer of ALPR data.
- The length of time the ALPR data will be retained and the process used to determine if and when to destroy retained ALPR data.

Agencies may expand on these required elements as needed to ensure that their collection, use, maintenance, sharing, and dissemination of ALPR data are consistent with respect for individuals' privacy.

None of the four agencies we reviewed have an ALPR policy that contains all of the required information, thereby contributing to the agencies' failure to implement programs that reflect the privacy principles in SB 34. Los Angeles has not developed an ALPR policy, and the policies of the other three agencies are deficient in various ways, as Figure 2 shows. For example, all have failed to fully address how they will monitor system use to ensure compliance with applicable privacy laws, which likely contributed to their failure to institute regular audits of user searches. The agencies could have avoided concerns such as those shown in Figure 2, which we describe later in this report if they had developed more thorough policies. Clear policies that define the purposes and procedures for monitoring ALPR systems help agencies meet their goals.

Figure 2
The Agencies' ALPR Policies Are Missing Required Key Elements for Respecting Individuals' Privacy



Source: State law and the agencies' ALPR policies as well as interviews with the agencies' management.

As a result of our audit, each of the four agencies is making or considering changes to its policies. The ALPR administrators at Fresno, Marin, and Sacramento agreed that their policies did not contain one or more elements required by state law. They also explained that they did not include certain policy requirements they believed did not apply to their use of ALPR data. For example, Sacramento's ALPR policy does not describe ALPR data-selling restrictions because, according to the ALPR administrator, Sacramento does not currently sell ALPR data. However, because their policies are incomplete and do not specify what personnel cannot do when interacting with their ALPR systems, these three agencies left out critical guidance to staff and increased the risk that staff would use the ALPR system inappropriately. The program administrators at Fresno, Marin, and Sacramento told us that they will consider changes to their policies subsequent to our audit. Although the lieutenant who serves as Los Angeles' program administrator initially believed that the agency's many IT policies covered the ALPR program, when we brought the deficiencies in oversight to his attention, he acknowledged the need for Los Angeles to have an ALPR policy and began drafting one in October 2019.

Fresno, Marin, and Sacramento have incomplete ALPR policies, which increases the risk that staff will use the ALPR systems inappropriately.

We are concerned that the policy deficiencies we found are not limited to the agencies we reviewed, and thus law enforcement agencies of all types may benefit from guidance to improve their policies. We surveyed 391 police and sheriff departments statewide about their ALPR programs, and many stated that they have ALPR policies and that these policies are publicly available. Because state law requires each agency that operates or uses an ALPR system to implement a usage and privacy policy, and to make the policy available to the public in writing and post it conspicuously on the agency's website, we inquired about how agencies throughout the State were adhering to these requirements. Of the law enforcement agencies using an ALPR system, 96 percent responded that they have ALPR policies. Of this group, at least 70 percent stated that they have posted their policy to their website. A breakdown of the law enforcement agencies' responses to our survey can be found at http://auditor.ca.gov/reports/2019-118/supplemental.html. However, we believe it is likely that many of the survey respondents will have the same problems with the quality and completeness of their policies as the four agencies we visited. As we discuss in the Introduction, Justice has issued guidance to law enforcement agencies to help them understand how to adhere to state law regarding the sharing of information for immigration enforcement purposes. Given Justice's experience and broad reach in the law enforcement community, developing guidance for local law enforcement agencies on needed policy elements could improve the quality and completeness of their policies.

The Law Enforcement Agencies Have Often Placed Their ALPR Data at Risk

Administering ALPR programs in ways that respect individuals' privacy requires a thoughtful and considered approach to data management that the agencies we reviewed have not always taken. Specifically, three of the agencies have agreed to share their images widely with little knowledge of the receiving entities and their need for the images. Moreover, the agencies have not based their decisions regarding retention of images on their actual usefulness to investigators and may be retaining the images longer than necessary, increasing the risk to individuals' privacy.

The Agencies May Not Be Adequately Protecting Their Sensitive ALPR Data

Law enforcement users can upload personal information and criminal justice information into the Vigilant system through hot lists and open text fields.

Law enforcement agency personnel can upload or enter sensitive information into their ALPR systems, which may require specific safeguards. As we discuss in the Introduction, this sensitive information could include personal information and criminal justice information. In addition, these data may originate from the California Law Enforcement Telecommunications System (CLETS)—a system that allows law enforcement agencies to obtain information from federal and state databases, such as arrests and fingerprint records from Justice. In reviewing multiple agencies' ALPR policies, we found several that stated that their ALPR systems may contain information obtained through CLETS. Additionally, in a security and compliance memorandum, Vigilant acknowledged that law enforcement users can upload personal information and criminal justice information into the Vigilant system through hot lists and open text fields.

For example, in addition to license plate images, Sacramento and Los Angeles add data to their systems such as criminal charges and warrant information, in combination with personal information such as names, addresses, dates of birth, and physical descriptions. The added data can be in the form of hot lists that agencies use to search for license plates of interest, as shown in Figure 1 in the Introduction, or they can be data that are entered into open text fields. By running an automated function each day, Sacramento extracts information from several databases and uploads the information as hot lists to its ALPR system. Los Angeles does not create its own hot lists, but it regularly downloads hot lists from Justice and the Los Angeles County Sheriff's Department, then uploads the hot lists to its ALPR system. Another way that information in addition to license plate images gets into an ALPR system is by users adding it to open text fields. Data entered into open text fields are generally associated with license plate searches.

When conducting a search, staff are prompted to enter a case number and the purpose of the search, and they may do so by typing in text. The ALPR systems store this open text in their audit logs, which detail user activity and the reasons for the activity.

In contrast to Sacramento and Los Angeles, Marin and Fresno occasionally upload hot lists into their ALPR systems. With regard to open text fields, we reviewed the audit logs for Marin and Fresno and did not find personal information in combination with other sensitive information in the six months of search records we studied. However, the possibility exists that law enforcement personnel could enter sensitive information into open text fields during ALPR searches.

When an IT system lacks sufficient security, the system is at risk of misuse and data breaches.

When an IT system lacks sufficient security, the system is at risk of misuse and data breaches. Systems containing personal information and criminal justice information must have adequate protections to assure individuals' privacy. However, as discussed in the Introduction, ALPR data can originate from different sources, and the source of the information may drive some of the required IT security protocols. On one hand, CJIS developed a policy that dictates the minimum standards that law enforcement agencies must follow to protect criminal justice information they obtain from the FBI (CJIS policy). On the other hand, users of Justice's CLETS system must follow the protections outlined in the CLETS *Policies, Practices and Procedures* document, which describes formal security measures law enforcement agencies must follow to access and protect CLETS information in addition to the CJIS policy requirements.

Further, it can be difficult to know what protections to apply to data from different sources. For example, an individual's address obtained by searching the Department of Motor Vehicles database through CLETS would be subject to Justice's data security requirements, but the same information obtained from a local law enforcement agency database would not. Moreover, the personal information Los Angeles and Sacramento have entered into their ALPR search records does not include its origin, making the required level of protection unclear.

Given these issues and the need to identify a standard that can be uniformly applied to ALPR data regardless of their source, we believe that CJIS policy provides reasonable security measures for law enforcement agencies to protect all of their ALPR data. State law requires these agencies to maintain reasonable security procedures and practices to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure. CJIS policy specifies operational, administrative, technical, and physical safeguards for each of these areas. For example, CJIS policy

requires agencies to ensure that their sensitive data are encrypted, and it limits physical access to specific personnel authorized to access the data. Nearly all of the 230 agencies that reported using ALPR systems in response to our statewide survey—including Fresno, Los Angeles, Marin, and Sacramento—reported that their ALPR data storage solution complies with CJIS policy.

We are concerned that the agencies using Vigilant may not be protecting their ALPR data in conformity with CJIS policy standards.

Nevertheless, we are concerned that the agencies using Vigilant may not be protecting their ALPR data in conformity with CJIS policy standards. Fresno, Marin, and Sacramento store their ALPR data in Vigilant's cloud database, and CJIS policy requires agencies to ensure that the cloud vendors that store and process their criminal justice information comply with its security requirements. Such requirements include controlling physical access to sensitive data, encrypting the data, and conducting background checks and training for employees with access to criminal justice information. In addition, before providing sensitive data to a vendor, CJIS requires law enforcement agencies to identify necessary authentication and monitoring controls, such as two-factor authentication and activity logging. Because the Vigilant software is by default accessible via the Internet, an officer may be able to access it using his or her personal device. The ability to access ALPR data in this manner bypasses the agencies' network security safeguards and violates CJIS policy requiring agencies to monitor and control access to the data.

One way to prevent users from signing in to the Vigilant system using personal devices would be to implement authentication controls, such as two-factor authentication. Two-factor authentication involves a second level of verification, such as a passcode sent to a specific device, and allows agencies to require that the passcode be sent only to department-issued devices. Although Vigilant offers two-factor authentication, Marin, Fresno, and Sacramento do not use it. CJIS policy requires two-factor authentication only for systems that directly access federal systems. However, this requirement recognizes that two-factor authentication is more secure than a basic username and password login for systems like Vigilant that are accessible over the Internet. Thus, two-factor authentication could serve as a best practice for agencies to prevent inappropriate access to their ALPR systems.

In addition, monitoring the activity logs can alert program administrators to unauthorized access of their ALPR systems. CJIS policy requires agencies to monitor access to systems that contain criminal justice information. Vigilant provides its clients with logs of network addresses that have accessed their ALPR systems, and although Marin's ALPR program administrator stated that he reviews these logs, administrators from Sacramento and Fresno confirmed that they do not. Reviewing the logs of system access

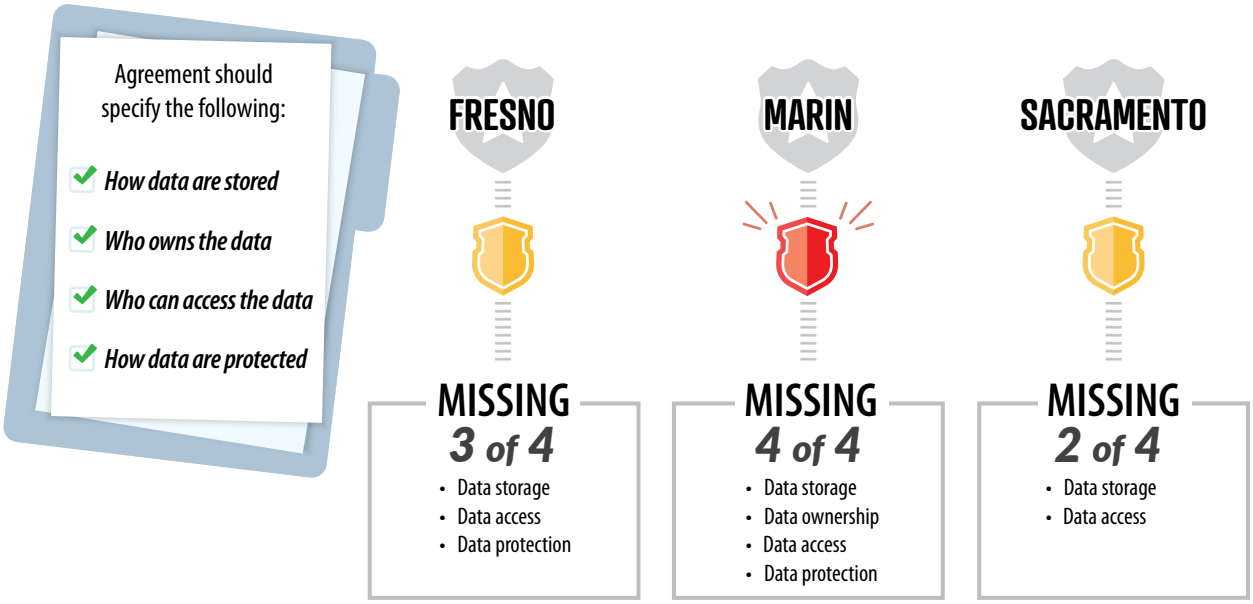
could help the agencies monitor access to their ALPR systems and detect whether someone accesses the ALPR system from an unrecognized network address.

When law enforcement agencies provide sensitive information to ALPR vendors, their contracts should provide assurance that the vendor will adequately protect that information. CJIS policy recommends several provisions that law enforcement agencies should consider including in their contracts to ensure that cloud vendors adequately protect criminal justice information. For example, a contract that protects a law enforcement agency's data would make clear that the agency owns the data it uploads into the ALPR system, that the agency's data will not be stored outside of the United States or Canada, and that employees at the cloud vendor who have access to unencrypted criminal justice information will undergo training and background checks. Without these contract provisions, agencies lack guarantees that the cloud vendor will implement appropriate protections of their data.

We found that the three agencies storing ALPR data in Vigilant's cloud—Fresno, Marin, and Sacramento—do not have sufficient data security safeguards in their contracts.

We found that the three agencies storing ALPR data in Vigilant's cloud—Fresno, Marin, and Sacramento—do not have sufficient data security safeguards in their contracts. As Figure 3 shows, none of the agencies' contracts with Vigilant meet all of the CJIS data security requirements. For example, the agencies' contracts do not state that Vigilant will store their data in the United States or Canada. Marin's contract does not make clear that Marin owns the data it adds to the ALPR system. It is important to note that Vigilant claims to implement data security measures that comply with CJIS policy. In a security and compliance memorandum, Vigilant lists steps it takes to encrypt data that may contain criminal justice information, as well as physical and network security safeguards it has in place to prevent unauthorized access to its ALPR cloud. We have no basis to dispute Vigilant's claims, but without strong contract provisions requiring CJIS safeguards, the three agencies have no guarantee that Vigilant will protect their data. As CJIS policy states, ambiguous contract terms can lead to controversy over data privacy and ownership rights, whereas a contract that clearly establishes data ownership acts as a foundation for trust that the cloud vendor will protect the privacy of the agency's data.

Figure 3
The Agencies' Existing Agreements With Vigilant Do Not Contain Adequate Data Security Measures



Source: Agencies' agreements with Vigilant and CJIS policy requirements.

A lack of IT department involvement and outdated contracts likely contributed to the data security weaknesses we observed. Fresno, Marin, and Sacramento have IT units that administer their systems and ensure compliance with Justice's data security requirements. However, at Fresno and Marin, the IT units are responsible for network security and have little oversight of the ALPR systems' data security. According to Fresno's IT manager, Fresno's main IT unit does not manage user accounts or monitor access to the ALPR system. Fresno has an IT analyst separate from the main IT unit who currently helps administer user accounts and provides technical support for the ALPR system; however, his background is not in network security. A deputy in Marin's auto theft unit manages Marin's entire ALPR system—including user accounts and training. This arrangement is not ideal, since individuals outside of an agency's IT department may lack the expertise necessary to implement adequate data security safeguards. According to Sacramento's ALPR administrator, Sacramento's IT unit recently assumed responsibility for the ALPR system, but before about April 2019, an officer outside of the IT unit administered the ALPR system.

In addition, with the exception of Sacramento, the agencies have not updated their contract terms with Vigilant for several years. The agencies' contracts renew each year when the agencies pay a service fee to Vigilant. As a result, Fresno has not updated its contract for three years, and Marin for nine years. Sacramento updated

its contract terms with Vigilant in September 2019, after using its previous agreement for seven years. Agreements that are not kept current may reflect outdated practices or omit needed assurances, increasing the risk that data are not protected.

Los Angeles was not able to demonstrate that it has an agreement in place to protect its ALPR data from inappropriate access.

Los Angeles was not able to demonstrate that it has an agreement in place to protect its ALPR data from inappropriate access. Los Angeles stores its ALPR data in a city-controlled data center rather than in a vendor cloud like the agencies that use Vigilant. Nevertheless, Los Angeles contracts with Palantir for IT support, and the FBI's 2017 audit of Los Angeles' data security practices identified Palantir as an entity with access to criminal justice information; thus we expected Los Angeles' agreement with Palantir to meet CJIS policy requirements. CJIS policy requires agencies to enter into agreements with vendors that access their criminal justice information. The agreements are to include an FBI-drafted security addendum that outlines specific safeguards a vendor agrees to put in place to comply with CJIS policy and an acknowledgment by the vendor of the great harm that may arise from misusing sensitive data. However, in response to our request for its agreement with Palantir, Los Angeles produced two expired contracts and a 2018 commodities agreement extending its licensing and support for Palantir software. None of these documents contained the FBI-drafted security addendum. Thus Los Angeles was not able to demonstrate that its agreement with Palantir contains appropriate data protections to ensure that Palantir employees with access to Los Angeles' ALPR data will not use the data for unauthorized purposes.

The Agencies Have Not Made Informed ALPR Image-Sharing Decisions

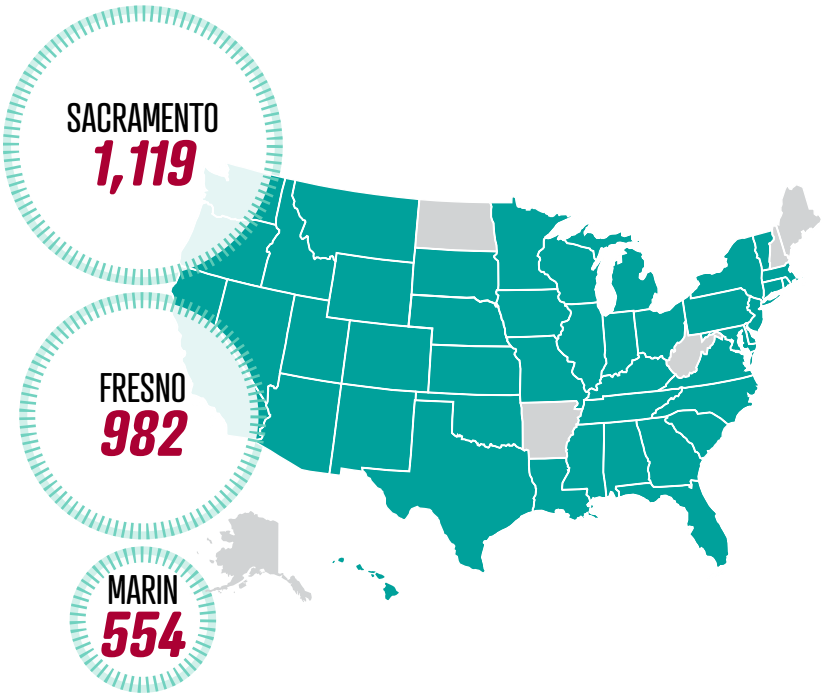
A significant feature of ALPR systems is their ability to share information with users across other organizations. A variety of requirements and guidance exist regarding how law enforcement agencies should share ALPR data, including images. ALPR images contain the date, time, and location of the scanned license plate and largely relate to vehicles that are not linked to crimes. The risk that the images will be misused rises as the images are more widely distributed, and there are numerous examples of law enforcement officers misusing their access to various databases. For example, an Associated Press article from 2016 reported a case from the state of Georgia in which an officer accepted a bribe to search for a woman's license plate number to see whether she was an undercover officer. Although such an example of misconduct is not representative of all law enforcement personnel, it illustrates the need for appropriate safeguards over law enforcement tools. Once a license plate is tied to an individual's identity, which is easy for a law enforcement officer to do, ALPR images may make it possible to track that individual's movements.

State law allows local law enforcement agencies to share ALPR images only with public agencies and requires sharing to be consistent with respect for individuals' privacy. Further, guidance that Justice issued in October 2018 addresses the agencies' governance of databases in relation to immigration enforcement, and this guidance provides a best practice for sharing in general. In the guidance, Justice encourages law enforcement agencies to inquire regarding the purpose for which an agency seeking access to their database intends to use the information and then, as a condition for accessing the database, to require agreements ensuring appropriate use of the data if its purpose includes immigration enforcement. The chiefs' association also recommends that law enforcement agencies maintain ALPR image-sharing records that include information on how the requester intends to use the images. The four agencies we reviewed asserted that they share ALPR images with others on the principle that these entities have a right and need to know the information. Because following state law necessitates establishing an agency's identity, i.e., the right to know, and Justice's guidance suggests establishing the purpose, i.e., the need to know, for which an agency intends to use the images, the agencies' position seems consistent with state law and Justice's guidance.

However, we had difficulty determining whether the reviewed agencies have actually made informed decisions about sharing their ALPR images. Fresno and Marin have each approved sharing their ALPR images with hundreds of entities, and Sacramento with over a thousand. Many of these entities are within California, but they also span most of the other 49 states. Figure 4 shows the entities' locations, illustrating how widely distributed access to these ALPR images is. In addition, we could not always ascertain how the agencies determined whether an entity receiving access to images had a right and need to access them or even whether the entity was a public agency. We reviewed the lists of entities and found one that appeared to be a non-public entity and others that were unidentifiable because they were listed only by initials. For example, Fresno, Marin, and Sacramento all approved an entity listed as the Missouri Police Chiefs Association (Missouri Association); however, this is not a public agency but rather a professional organization that provides training opportunities and advocates for pro-law enforcement legislation. However, none of the agencies could demonstrate that they had evaluated the Missouri Association before sharing images, nor could they tell us why the Missouri Association had a right to those images. When we inquired with Vigilant, an official explained that despite the name, it is the Missouri State Highway Patrol—a law enforcement agency—that uses the account. The lists contain many other entities whose identities and law enforcement purposes are not immediately evident. Unless a law enforcement agency verifies each entity's identity and its right to view the ALPR images, the agency cannot know who is actually using them. Although the three agencies reviewed their sharing arrangements to varying degrees during our audit, none could demonstrate that they perform this kind of verification before sharing their ALPR images.

We could not always ascertain how the agencies determined whether an entity receiving access to images had a right and need to access them or even whether the entity was a public agency.

Figure 4
Three Agencies Have Authorized Sharing With Entities Located in States Across the Nation



Source: Analysis of data-sharing reports from the Vigilant system.

Similarly, even when an entity is a verified public agency, it is not always evident that agencies are making informed decisions by establishing the entity's need for the ALPR images. Fresno, Marin, and Sacramento all authorized sharing with the Honolulu Police Department, but given the distance between California and Hawaii and the limited instances of cars traveling between the two states, it is uncertain whether the Honolulu Police Department has a persuasive need for these ALPR images. Fresno's ALPR administrator agreed that not a great deal of thought went into its decision to share with the Honolulu Police Department, and he believes that it probably authorized the share because the entity was a law enforcement agency. In contrast, Marin's ALPR administrator believes that sharing ALPR images widely is important because the more information available to law enforcement, the more successful it can be in its mission. However, sharing decisions should also consider the importance of protecting individuals' privacy. Each authorized share exposes the ALPR images to greater risk of misuse; therefore, the agencies should approach each sharing request individually based on the requester's actual need for the images.

The three agencies have also relied on features in Vigilant's software rather than establishing their own practices for sharing their ALPR images. A sound approach to sharing would include establishing each requesting entity's need to know and right to know and keeping records of the assessment and resulting decision. However, none of these agencies maintain records outside of the Vigilant user interface of when or why they agreed to share with particular entities, and neither Marin nor Sacramento includes a process for approving sharing requests in their ALPR policies as state law requires. Fresno has outlined procedures that incorporate these elements, but it has not followed them. Fresno's ALPR administrator explained that its procedures require more information than an entity requesting a share provides in the Vigilant user interface, and there has been frequent turnover in the position responsible for approving sharing requests.

Current administrators at the three agencies have difficulty understanding when and how sharing occurred because the information the Vigilant user interface displays has changed over time. The status of a sharing relationship in the Vigilant system depends on whether the involved entities' accounts are *active* or *inactive*. Active entities have a current account with Vigilant while inactive entities do not. An agency may agree to share with an active entity that later becomes inactive. Images cannot be shared between active and inactive entities. However, unless an agency deliberately removes a sharing relationship with an inactive entity, that sharing relationship remains and would become operational if an inactive entity decided to renew its account with Vigilant and become active once more. Previously, Vigilant had structured its user interface so that inactive entities did not appear in the sharing report that shows a list of entities with whom an agency had agreed to share. Recently, Vigilant changed its interface to make inactive entities visible. Whether an entity is active is not apparent from the sharing report alone.

A change in the vendor's user interface and not keeping records of authorized shares made it difficult for ALPR administrators to track current sharing relationships.

This change in the user interface and the fact that agencies kept no records of the shares they have authorized made it difficult for ALPR administrators at the agencies to know the status of current sharing relationships. For example, in 2014 a prior ALPR administrator for Marin had agreed to share images with three U.S. Immigration and Customs Enforcement (ICE) agencies. In December 2018, Marin's current ALPR administrator used the Vigilant user interface to review the sharing report and noted that the report included no ICE agencies. However, when he reviewed the report again in August 2019—at our request—three ICE agencies appeared on the list. We discussed this discrepancy with Vigilant, which explained that the three ICE agencies were currently inactive. When Marin's ALPR administrator reviewed the sharing report in December 2018, inactive agencies did not appear on the report, but Vigilant subsequently changed its user interface so that inactive

agencies did appear. Although the ICE agencies could not access Marin's ALPR images because they were inactive, to effectively end the share, Marin needed to remove the authorization for sharing with the ICE agencies, which Marin has since done.

According to Marin's ALPR administrator, it is now the department's position that it will not share images with ICE, but if it had remained unaware that the sharing relationships existed and the ICE agencies had become active again, it would have been sharing its ALPR images with them without knowing it was doing so. Had Marin kept its own records of the sharing to which it had agreed, it would have been aware that it had agreed to share with ICE in the past, and it would have been able to remove those shares promptly. Sacramento had also authorized sharing to ICE agencies in the past. When the current ALPR administrator reviewed the list of entities with which it shared images with in response to our audit, he removed those shares as well. In contrast, Fresno had never authorized any sharing relationship with an ICE agency.

Although none of the agencies using Vigilant currently share with ICE agencies, all three had authorized shares with entities with border patrol duties. Despite not having implemented any agreements related to this sharing since Justice issued its guidance in October 2018, the three agencies were all sharing with the San Diego Sector Border Patrol of U.S. Customs and Border Protection at the start of our audit. During our audit, Sacramento removed the share to this agency. Marin and Sacramento had also authorized sharing with an agency listed as "California Border Patrol," and although Sacramento removed this share at the same time it removed the shares to ICE, Marin continues to share with this entity. Fresno continues to share with the Customs and Border Protection National Targeting Center. Although Sacramento had also authorized a share to this entity, it removed this share during our audit. All of these entities' duties could potentially intersect with immigration enforcement. Justice's guidelines for sharing data are particularly relevant in these cases, yet the agencies were either unaware of these guidelines or had not implemented them for their ALPR systems.

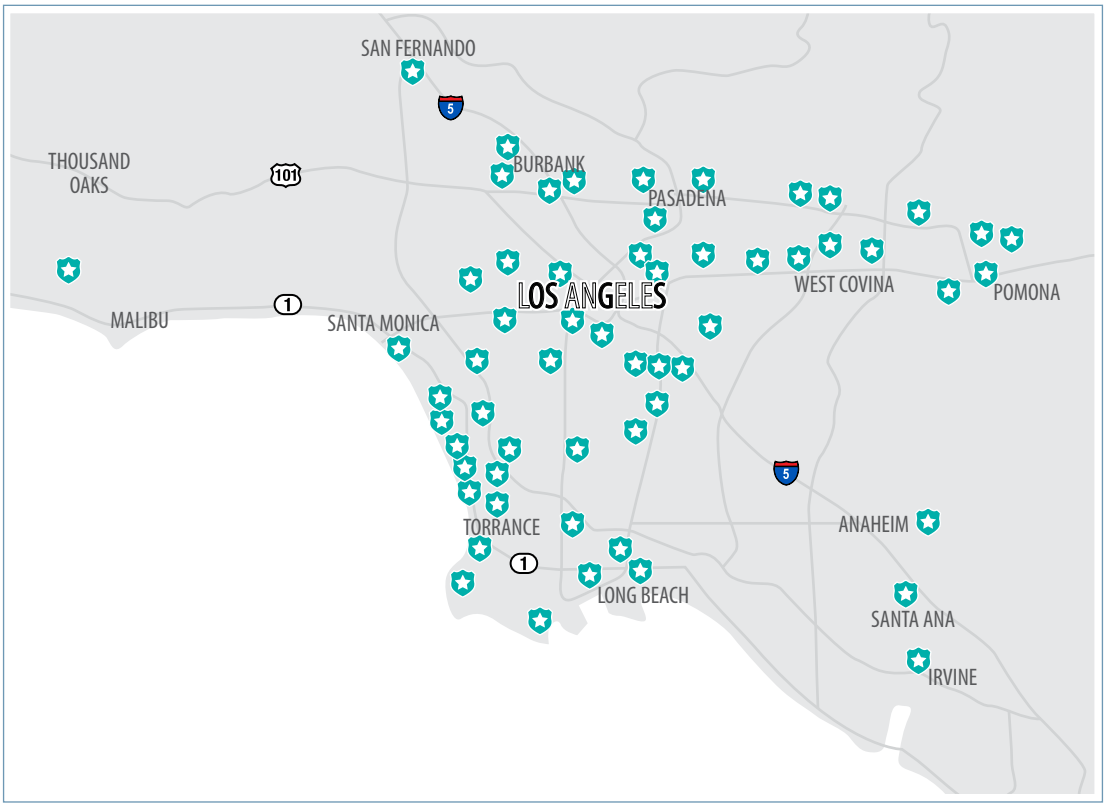
Justice's guidelines for sharing data are particularly relevant, yet Fresno, Marin, and Sacramento were either unaware of these guidelines or had not implemented them for their ALPR systems.

Of the four agencies we reviewed, only Fresno and Sacramento share hot lists they create, and they do so through a more controlled process than for sharing ALPR images. Vigilant's user interface enables hot-list sharing in addition to sharing ALPR images. In contrast to its wide sharing of ALPR images, Fresno shares the hot lists it occasionally uploads with only three law enforcement agencies in the nearby region. Sacramento has agreed to share six hot lists with eight law enforcement agencies in California. With each agency, Sacramento took the additional step of developing a memorandum of understanding providing guidelines for sharing the hot lists and the signature of the chief official at each agency.

Although the memorandum does not specify which hot lists Sacramento will share, it does provide a record of the entities with which hot-list sharing occurred, unlike its sharing of ALPR images for which no independent records exist outside the Vigilant user interface.

In contrast with the other reviewed agencies, Los Angeles has limited its sharing of ALPR images to entities within a regional structure established for its ALPR program through a federal grant that helped fund its ALPR program. As Figure 5 shows, Los Angeles shares ALPR images with 58 other law enforcement agencies in the region. It does not have agreements to share its ALPR images with any federal agencies, including ICE. According to the lieutenant who administers the ALPR program, Los Angeles decided to share images only with entities using the same software so that it could maintain greater control over its ALPR images. It has a formal agreement with each agency, which provides a record of its sharing decisions.

Figure 5
Los Angeles Shares Images With 58 Law Enforcement Agencies



Source: Analysis of data-sharing memorandums of agreement.

The Agencies' Image Retention Decisions Are Unrelated to How They Use the Images

The four agencies we reviewed retain ALPR images for varying periods of time. Our review determined that with the exception of CHP, state law does not mandate a specific retention period for ALPR images collected, accessed, or used by public agencies, nor does state law delineate the factors public agencies should use in determining those periods. Instead, state law requires that public agencies other than CHP that use or operate ALPR systems specify, in the agency's usage and privacy policy, the length of time ALPR data will be retained and the process that the agency will use to determine if and when to destroy retained ALPR data. Fresno's policy is to retain ALPR images for a minimum of one year, Sacramento's policy is to retain ALPR images for a minimum of two years, and Marin's policy is to retain images for two years. Although the agencies' policies describe their retention periods as minimums, in practice the agencies have configured their ALPR systems to delete images older than their specified retention periods. Fresno and Sacramento each download and retain images for longer than their prescribed retention policies if the images are relevant to investigations. Los Angeles does not have an ALPR policy, but the lieutenant who administers the ALPR program stated that it adheres to the city's Administrative Code, which requires data to be retained for a minimum of five years.

None of the agencies considered the images' utility over time when establishing their retention periods.

None of the agencies considered the images' utility over time when establishing their retention periods. Fresno based its ALPR image retention period on state law, which allows some cities to destroy certain video monitoring records after one year. Marin did not cite state law in its policy; its former ALPR administrator stated that when setting a two-year retention period, he considered other agencies' retention periods and the retention requirements for litigation related to investigations. Both Marin's and Fresno's ALPR administrators stated that they were not aware of any studies of how useful older images in their ALPR systems were to their personnel. In its ALPR policy, Sacramento cited a general state law that prohibits some cities from destroying records less than two years old. The lieutenant who oversees Sacramento's ALPR program acknowledged that the agency has not conducted any statistical analysis to determine how long it needs to retain ALPR images. However, he stated that, although he was not involved in drafting the original policy, two years made sense considering federal regulations, which permit retention of criminal intelligence information for no longer than five years. The lieutenant cited those federal regulations as a best practice for retaining sensitive data, connecting the ALPR images to a tenet of federal regulations that law enforcement agencies should keep criminal intelligence information as long as it is useful, even though ALPR data are not criminal intelligence.

To develop a retention policy that better protects individuals' privacy, an agency might begin by considering the time period during which ALPR data are most useful to law enforcement. To assess the usefulness of these images over time, we reviewed the four agencies' ALPR searches over a six-month period—between late January and September 2019, depending on when we visited the agencies—and found that personnel at three of the four agencies typically searched for ALPR images zero to six months old. When searching ALPR systems, investigators can enter search dates to target specific periods of interest. For example, on March 29, 2019, a Sacramento investigator searched for ALPR images from six days earlier—March 23—indicating that images less than one week old were relevant to that search. As Table 2 shows, we found that the searches agency personnel at the three agencies performed infrequently included older images. In fact, when investigators at Fresno, Marin, and Sacramento specified date ranges, most searches were of ALPR images that were less than six months old. In contrast, Los Angeles had a relatively even distribution of searches between those less than one year and those more than one year old. The Vigilant system defaults to showing the 50 most recent records when investigators do not specify a search date range. We analyzed 46,000 records for searches that did not specify a date range and found that investigators for Marin, Fresno, and Sacramento frequently did not seek further than the 50 default records, indicating that they generally were not interested in older ALPR images.

Table 2
The Agencies Usually Search for ALPR Images That Are Six Months Old or Less

			PERCENTAGE OF SEARCHES FOR IMAGES OF A SPECIFIED AGE			
	RETENTION PERIOD	TOTAL SEARCHES OVER 6-MONTH PERIOD ANALYZED	0 TO 6 MONTHS	6+ MONTHS TO 1 YEAR	1+ TO 2 YEARS	MORE THAN 2 YEARS
Fresno*	1 year	850	92%	6%	1%	1%
Los Angeles	**5 years**	28,874	42	8	29	21
Marin*	2 years	26	88	8	0	4
Sacramento*	2 years	4,262	84	4	11	1

Source: Analysis of search records from the agencies' ALPR systems between late January and September 2019, depending on when we visited the agency.

* The percentage of searches listed in this table beyond an agency's retention period are likely from their personnel searching data belonging to other agencies with longer retention periods.

Other states have established retention periods that are generally shorter than the lengths of time California's local law enforcement agencies are retaining ALPR images. The National Conference of State Legislatures identified at least 13 states that mandate maximum ALPR image retention periods. As the text box shows, these vary widely, from three minutes in New Hampshire to three years in Florida. Nevertheless, the majority of these states have retention periods that do not exceed six months.

In contrast, 230 California agencies responding to our survey reported that they use ALPR systems, and nearly 80 percent of these—180 agencies—stated that they retain their ALPR images for more than six months. About 20 of those agencies indicated that they retain ALPR images for more than five years. Figure A.2 in Appendix A summarizes these responses.

ALPR Image Retention Periods for 13 States

New Hampshire	***3 minutes***
Maine	21 days
Minnesota	60 days
Montana	90 days
North Carolina	90 days
Tennessee	90 days
Arkansas	150 days
Nebraska	180 days
-------- LONGER THAN SIX MONTHS --------	
Utah	270 days
Colorado	365 days
Vermont	540 days
Georgia	900 days
Florida	***3 years***

Source: National Conference of State Legislatures, *Automated License Plate Readers: State Statutes,* March 15, 2019, and review of the listed states' ALPR laws and guidelines.

Note: These states allow retention for longer periods for specific reasons, such as data used in investigations.

The length of time law enforcement agencies need to retain ALPR images will vary depending on how they use the images. Narrow use—for one purpose only, such as locating stolen cars—could dictate a short retention window. Personnel we interviewed at each of the four agencies stated that investigators rely primarily on recent images to investigate some types of crimes, such as auto theft. In contrast, using ALPR images to solve complex crimes could necessitate a longer retention window. For example, first-degree murder can be prosecuted at any time; therefore, a homicide investigator may be able to use ALPR images of any age to help solve a case. The four agencies we reviewed have access to information they can use to evaluate whether their ALPR retention periods are reasonable. Their systems record each time personnel search ALPR images, and these search records show the date of the search and the parameters used to narrow the search, such as location, date, and time. Agency administrators can analyze these activity logs to understand the images personnel are searching for and their relative ages.

Marin and Sacramento have allowed expired hot lists to remain in their ALPR systems for far longer than their specified retention periods. Unlike ALPR images, hot lists cannot be automatically deleted by the Vigilant system. Instead, the agencies define a period after which the hot list becomes inactive—meaning the ALPR system no longer generates alerts from the list—but the list remains stored in Vigilant's servers until the agency deletes it. We found that Marin and Sacramento are retaining hot lists longer than necessary because their administrators were unaware of the need to manually delete them. They assumed that their Vigilant system would automatically delete inactive hot lists according to the designated purge schedule, as it does ALPR images. For example, Marin retained an inactive hot list of sex offenders for five years—three years longer than its two-year retention period for ALPR images. Sacramento has retained multiple hot lists for as long as six years—four years longer than its retention period for ALPR images. The types of lists ranged from a hot list of Sacramento County sex offenders to a warrants hot list. When we brought the inactive hot lists to the agencies' attention,

the administrators at Marin and Sacramento acknowledged that the age of the hot lists exceeded the agency's retention period, and they were willing to delete the hot lists.

Law enforcement agencies should consider both the usefulness of the ALPR images and individuals' privacy when deciding how long to retain the images. Cost, however, is not a factor. According to the lieutenant who oversees Los Angeles' ALPR program, the images are useful to investigators and the cost of storing ALPR images is not a significant factor in determining how long to store them. Nevertheless, two studies by a consultant to the National Institute of Justice and the chiefs' association concluded that law enforcement agencies must consider the trade-offs between privacy concerns and the utility of retaining the ALPR images they capture and store.

The Law Enforcement Agencies Have Failed to Monitor Use of Their ALPR Systems and Have Few Safeguards for Creating ALPR User Accounts

Instead of ensuring that only authorized users access their ALPR data for appropriate purposes, the agencies we reviewed have made abuse possible by neglecting to institute sufficient monitoring. ALPR systems should be accessible only to employees who need the data and who have been trained in using the system. However, the agencies often neglected to limit ALPR system access, to provide appropriate training to individuals with access, or to monitor accounts. Similarly, to ensure that individuals with access do not misuse the system, the agencies should audit the license plate searches users perform. Instead, the agencies conduct little to no auditing and thus have no assurance that misuse has not occurred.

Best Practice Safeguards for Establishing and Managing User Accounts

Account Setup

- Supervisor approval is a prerequisite for account access.
- ALPR training is a prerequisite for account access.

Account Maintenance

- Accounts defined as *inactive* are suspended.
- ALPR training is required for users linked to inactive accounts to regain active status.
- Accounts are deleted when employees separate from the agency.

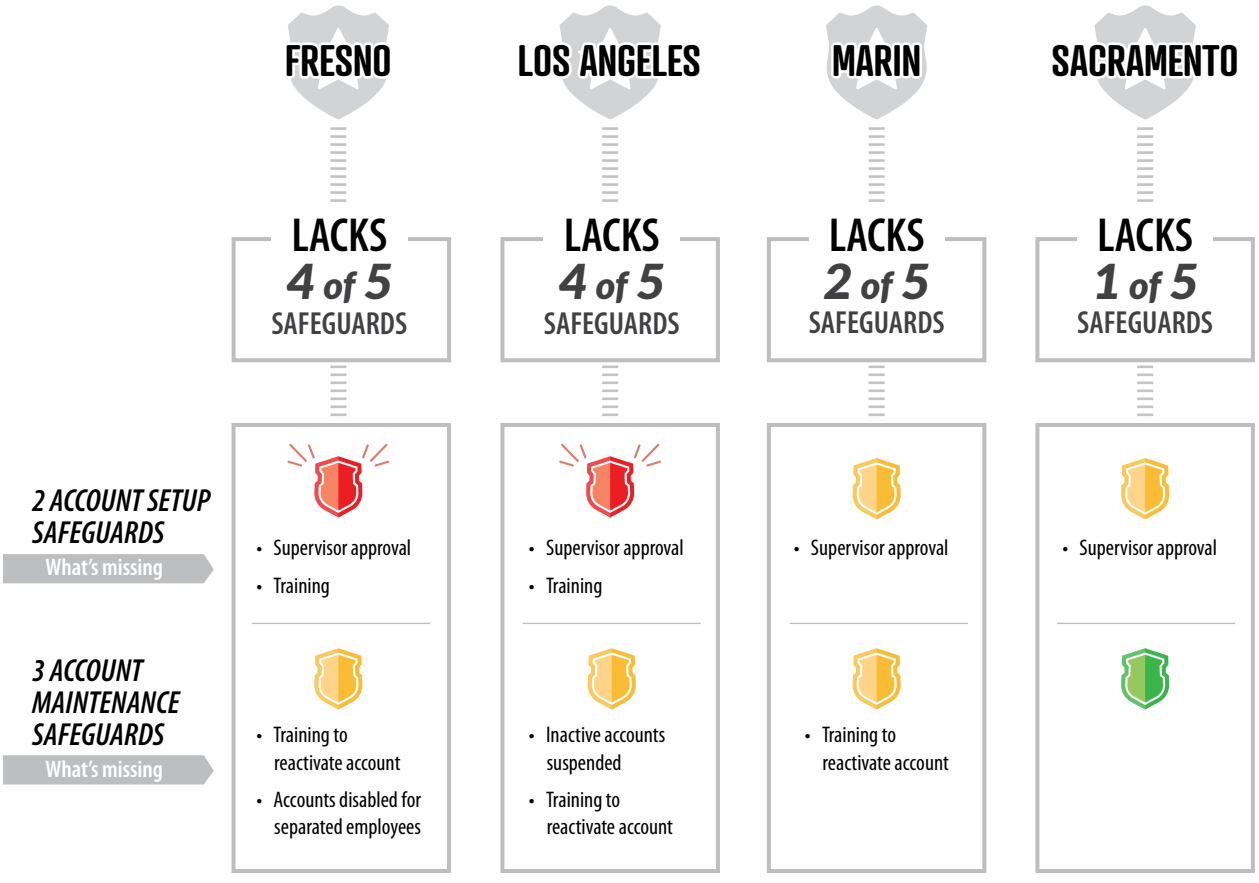
Source: CJIS policy and the *State Administrative Manual*.

The Agencies Need Stronger User-Access Safeguards

The four agencies we reviewed all failed to follow one or more best practices related to user access. State law requires agencies to maintain reasonable security procedures and practices to protect ALPR data from unauthorized access, and the text box lists five best practices for user access, from initiating an account to disabling it when an employee separates from the agency. Figure 6 shows the four agencies' status in implementing these best practices. Each ALPR administrator stressed the concept of "need to know, right to know" as a key for data security; however, no agency followed all of the best practices that would help establish the need to know and right to know. For example, no agency had a requirement

that supervisors approve staff requests for creating ALPR user accounts. Such a step would provide assurance that the staff member receiving the account had both a need and a right to access the information in the ALPR system. Los Angeles is particularly lax in this area because the protocol of its IT division is to include its ALPR software on each computer it assigns to staff, regardless of their position. Thus, staff who do not perform functions related to the ALPR system nevertheless have access to the system. In contrast, Sacramento follows all but one of the best practices listed in the text box. In doing so, it requires staff to prove their initial and continued need for ALPR data, among other access requirements.

Figure 6
The Agencies Lack Many Best Practice Safeguards for Establishing and Managing User Accounts



Source: Agencies' policies, applicable procedures and protocols, and interviews with the agencies' management.

Agencies could reduce instances of unnecessary access by ensuring that only those staff whose current work assignments require access to ALPR data have that access. The ALPR administrators at Marin and Los Angeles believe that supervisory approval is unnecessary

because ALPR users are already privy to data they consider more confidential than ALPR data, such as criminal justice information. However, these views do not consider that ALPR systems capture images indiscriminately, irrespective of the criminal history of the individual who is driving the vehicle, and the images allow law enforcement to track individuals. Given that agencies retain these images for several months or years, a user could combine them with personal information from separate data sources to produce a great number of details about someone's life, such as his or her political or religious affiliation. Without proper safeguards, staff could conduct this form of surveillance on any driver. In fact, the chiefs' association acknowledged this possibility and warned that increasing ALPR use and data sharing would enhance the potential for surveillance. Thus, as the chiefs' association concluded, limiting ALPR access to employees with the needs and the rights to access these data is a good step toward protecting the individuals whose privacy would be violated if the data were misused.

Limiting ALPR access to employees with the needs and the rights to access these data is a good step toward protecting the individuals whose privacy would be violated if the data were misused.

Ensuring that ALPR users are properly trained is another weakness among the agencies we reviewed. Three of the agencies do not ensure that all of their ALPR users are properly trained. The chiefs' association called the training of authorized ALPR users "a critical accountability measure." However, as Figure 6 shows, neither Fresno nor Los Angeles requires all ALPR users to complete ALPR training before initially obtaining system access. Although Los Angeles offers ALPR training, the detective who conducts this training confirmed that it is not required before users can access the ALPR system. Fresno's policy encourages such training; however, its ALPR administrator confirmed that the agency does not provide training to all of its users. Further, Marin's ALPR administrator stated that although Marin provides training when staff first receive access to the ALPR system, it does not require staff to renew their training in order to reactivate their accounts following long periods of not using the system. Without sufficient training, there is little assurance that ALPR users know and understand agency ALPR policies, including recent changes, or are aware of the limits on how they may use ALPR data.

Although the Fresno ALPR administrator agrees that the agency's safeguards surrounding user access are currently inadequate and plans to improve them, the ALPR administrators at Los Angeles, Marin, and Sacramento believe their current practices are acceptable. The administrators at Marin and Los Angeles are reluctant to alter their agencies' existing practices because they believe ALPR data are not as sensitive as other law enforcement data. We disagree with these views because, as we mention previously, ALPR data are sensitive and state laws require reasonable security procedures and practices to protect them. A basic protection for data that must be treated as sensitive is to limit who can access them.

In addition, as we mention earlier, the ALPR images law enforcement agencies collect largely involve vehicles that are not associated with crimes, and if the images were analyzed, the data could reveal behavior patterns and preferences that law enforcement could use to conduct surveillance on individuals. For example, according to a 2012 newspaper article, the New York Police Department collected license plate numbers of vehicles parked near a mosque. The department was purportedly trying to identify terrorist activities. Although the department justified this data collection as part of its strategy to identify potential criminal activities, it targeted mosques and collected license plate numbers at times without any leads or proof of terrorist connections. Given the sensitivity of the information collected in this example, access safeguards would ensure that only those staff who have a need and right to access an ALPR system would possess that privilege.

Law enforcement agencies could further improve safeguards by disabling employees' accounts once they separate or after long periods of nonuse. We reviewed Marin's and Sacramento's processes for disabling accounts of separated employees. Both agencies follow a similar approach, relying on one part of the organization providing information to another. Sacramento produces a personnel transfer and separation list every two weeks, and the IT security group uses it to identify accounts to close. Although the IT security group generally disabled accounts promptly after receiving the list, we found that the contents of the list were not always current. For example, in one instance, a separated employee did not appear on the list until 46 days after his separation date in June 2019. According to a human resources specialist, employees submit their resignation paperwork late at times, which causes human resources to not process this paperwork until after an employee has left the department. Marin's ALPR administrator said that he removes ALPR accounts once he receives a department-wide email notifying him of an employee's resignation or termination. He also stated that he checks ALPR accounts every few months to verify that active accounts match active employees. However, for one employee, the administrator did not disable his ALPR access until two months after he resigned in October 2019. In fact, the administrator did not disable this employee's access until our office pointed out that the account was still active. The fact that Marin and Sacramento did not disable some accounts as necessary is problematic because the former employees could log into their accounts and access ALPR data from the web-based version of the ALPR systems on any Internet-capable device, not just office devices.

The fact that Marin and Sacramento did not disable some accounts as necessary is problematic because the former employees could log into their accounts and access ALPR data from the web-based version of the ALPR systems on any Internet-capable device, not just office devices.

With regard to Los Angeles and Fresno, Los Angeles' network manager described an automated process for deleting accounts linked to overall network access, which reasonably aligned with best practices. Conversely, Fresno's ALPR administrator said that

he periodically reviews the names of employees with user accounts but started doing so only in September 2019 when he learned of our audit. We did not test deleted accounts at either agency. Deleting accounts prevents separated employees from continuing to access ALPR data and is thus critical to protecting ALPR data and individuals' privacy.

The Agencies Have Failed to Audit ALPR Users' Searches to Ensure That Individuals' Privacy Is Protected

State law requires law enforcement agencies that operate, access, or use ALPR systems to protect their ALPR data—including ALPR images—from unauthorized access, destruction, use, modification, or disclosure. The law specifically requires them to describe and implement a policy detailing how they will monitor their ALPR systems. According to state law, agencies that access or use ALPR systems must also conduct periodic system audits. In its reports on managing ALPR systems, the chiefs' association stated that conducting audits aids in discouraging unnecessary or inappropriate use of the data; in addition, when agency policies include a strong auditing requirement, this reassures the public that their privacy interests are recognized and respected.

Even though law enforcement agencies that use or access ALPR systems can monitor searches simply by reviewing search records for red flags, they should also conduct audits as required by state law.

A primary form of auditing to prevent misuse is reviewing the searches users conduct in the ALPR systems. Users conduct searches for specific license plates. Even though law enforcement agencies that use or access ALPR systems can monitor searches simply by reviewing search records for red flags, such as an unknown user account, they should also conduct audits as required by state law. An audit entails a more rigorous approach, including evaluating risk and randomly selecting test items for review. Developing an audit of license plate searches, for example, would involve determining how many searches to review, how to select test items, and how frequently to conduct the audit. Law enforcement agencies have often found evidence of misuse of their databases, showing the need for auditing. For example, a news article reported that CHP investigated 11 cases of database misuse in 2018, including three involving officers improperly looking up information on license plates through CLETS without a need to know the information. The large datasets of ALPR images, dating back at least one year, that the four reviewed agencies maintain can be analyzed to reveal the daily patterns of vehicles that can be linked to individuals and their activities—most of whom have not engaged in criminal activity. A member of law enforcement could misuse ALPR images to stalk an individual or observe vehicles at particular locations and events, such as doctors' offices or clinics and political rallies. Despite these risks, the agencies we reviewed conduct little to no auditing of users' searches.

We asked key officials at the three agencies using the Vigilant system why they had not audited the searches users performed and found that either they were unaware of the auditing requirement in state law or the auditing they did conduct did not include user searches. Fresno's policy states that it should conduct audits on a regular basis, but the ALPR administrator told us he believed audits are the responsibility of the Audits and Inspections Division within the department. However, the sergeant responsible for audits and inspections—who took charge in January 2018—responded that he was not aware of the requirement until our audit. Similarly, the Marin ALPR administrator was unaware of the state law requiring audits of ALPR systems until our audit and thus had not been conducting them. At Sacramento, the policy states that the ALPR administrator will conduct periodic audits of user searches. Even though Sacramento administrators had been monitoring some system functions, they had not audited searches of the older ALPR images. The officer administering the ALPR program until April 2019 said that she did not conduct these audits because her predecessor had not informed her that it was necessary. The ALPR program transferred to a new division in April, and according to the current ALPR administrator, limited staff resources have prevented him from instituting these audits.

Although the agencies have not been conducting audits, we considered the possibility that an agency employee or member of the public may have reported instances of ALPR misuse. We searched each agency's records of internal affairs investigations from January 1, 2016, to the present for cases involving ALPR misuse and did not find any such cases. However, we do not consider this proof that no instances of ALPR misuse occurred. Given that the agencies were not regularly auditing their systems, ALPR misuse may have occurred and gone unnoticed and unreported.

All four agencies must address the quality of information they will need to audit user searches. In Sacramento, for 66 percent of searches, users left case number and search reason fields blank.

To engage in meaningful auditing of their system users, all four agencies need to address the quality of the information users enter into the system as part of their searches. Before allowing users to conduct searches, Fresno, Los Angeles, and Marin require users to enter case numbers and reasons for the search; however, this is not happening consistently. We reviewed six months of user queries at the three agencies and found that users entered a wide variety of information in the case number field. For example, users at Los Angeles simply entered "investigation" into this field as well as descriptions of vehicles and actual case numbers. In contrast, Sacramento does not require users to enter either case numbers or reasons. Our review showed that in 66 percent of searches, Sacramento's users left both fields blank. When users fail to enter any information or fail to include appropriate detail, identifying misuse through audits becomes nearly impossible.

Los Angeles faces additional hurdles in performing meaningful auditing because its ALPR administrators do not have immediate access to data on user searches. Instead, according to the chief data officer, administrators need to request that a software engineer from Los Angeles' ALPR software contractor build and run a query in the system to obtain these data. In 2015 Los Angeles recognized a need to fix this software limitation to enable administrators to audit user searches. The chief data officer for Los Angeles stated that, although an initial upgrade provided an audit dashboard tool for administrators, subsequent software upgrades made this tool unusable, and the company that provides the software is developing a new one. He said that it is Los Angeles' goal to have a new audit dashboard tool by the end of the first quarter of 2020, at which point he will work with the appropriate division within the department to develop an audit plan. Although we agree that an audit tool will facilitate audits, we believe it was entirely possible for Los Angeles to obtain the data on user searches, and thus it could have implemented a process for periodic system audits as state law requires, despite the difficulties.

Fresno, Marin, and Sacramento do not have adequate policies or processes in place for conducting meaningful audits.

The other three agencies also do not have an adequate policy or process in place for conducting meaningful audits. For example, Fresno's ALPR policy states that it should conduct periodic audits, but its policy does not specify how frequently it will audit its ALPR system, who will perform those audits, who will review and approve the audit results, and how long it will retain the audit documents. Specifics such as these provide a clear road map for planning, conducting, documenting, and resolving audits. When followed, the agencies will have records demonstrating their necessary oversight. Marin's latest policy—dated July 2019—also fails to cover these necessary details. Fresno and Marin began reviewing user queries subsequent to the beginning of our audit, but in the absence of an adequate policy or formal plan, their methodologies are lacking. For example, although Fresno began conducting audits that included a random sample of user searches, staff have not developed a formal plan and provided us only with handwritten notes on their methodology. Marin's ALPR administrator has not instituted audits and is simply monitoring license plate searches by looking for instances in which the user did not enter a reason for the search or entered a reason that does not make sense, such as an investigation that does not exist. In addition, at both Fresno and Marin, the individual conducting the audits or monitoring is also a system user, creating a conflict when acting as a system monitor or auditor. Without sound methodologies, the agencies cannot be confident that they have sufficient protocols in place to detect misuse.

Other Areas We Reviewed

To address all the audit objectives approved by the Joint Legislative Audit Committee (Audit Committee), we reviewed two additional subject areas: whether the agencies offered opportunities for the public to comment on their ALPR programs and whether the Sacramento County Department of Human Assistance (Human Assistance) continues to operate an ALPR program.

Three Agencies Provided Information to the Public on Their ALPR Programs

State law requires that public agencies implementing ALPR programs after January 1, 2016, offer an opportunity for the public to comment about those programs. These opportunities increase public awareness that law enforcement agencies are using electronic means to collect information about vehicles in the community and offer a way for the public to provide feedback about the programs. The four agencies we reviewed began using ALPR before 2016 and consequently were not required to offer an opportunity for public comments. Nonetheless, three of the agencies took some steps to communicate with the public about their ALPR programs. Los Angeles and Sacramento published documents describing their ALPR programs, and at a Fresno City Council meeting, the public had an opportunity to comment on the selected ALPR vendor before the council voted on a new contract. The minutes from that meeting reflect that the public made no comments. This transparency helps foster public trust in law enforcement and government as a whole.

Human Assistance No Longer Operates an ALPR Program

Our audit scope included reviewing the ALPR program of Human Assistance, which provides Sacramento County residents with employment assistance and supportive services. Human Assistance contracted with Vigilant for three years to access ALPR images. Human Assistance did not operate its own cameras, and it used the ALPR images to investigate welfare fraud. According to the administrator of its ALPR program, Human Assistance ended its program in 2018 after determining that investigative staff rarely searched the images, so the program could not justify the cost. On November 1, 2018, Human Assistance deleted its ALPR user accounts, leaving the administrator's account active for internal review. On May 31, 2019, Human Assistance's ALPR agreement with Vigilant expired, and the administrator no longer has access to the account. Therefore, we did not perform any additional audit work pertaining to Human Assistance.

Recommendations

Legislature

- To better protect individual's privacy and to help ensure that local law enforcement agencies structure their ALPR programs in a manner that supports accountability for proper database use, the Legislature should amend state law to do the following:
  - Require Justice to draft and make available on its website a policy template that local law enforcement agencies can use as a model for their ALPR policies.
  - Require Justice to develop and issue guidance to help local law enforcement agencies identify and evaluate the types of data they are currently storing in their ALPR systems. The guidance should include the necessary security requirements agencies should follow to protect the data in their ALPR systems.
  - Establish a maximum data retention period for ALPR images. The Legislature should also establish a maximum data retention period for data or lists, such as hot lists, that are used to link persons of interest with license plate images.
  - Require periodic evaluation of a retention period for ALPR images to ensure that the period is as short as practicable.
  - Specify how frequently ALPR system use must be audited and that the audits must include assessing user searches.
  - Specify that those with access to ALPR systems must receive data privacy and data security training. The Legislature should require law enforcement agencies to include training on the appropriateness of including certain data in an ALPR system, such as data from CLETS.

Law Enforcement Agencies

- To ensure that their ALPR policies contain all of the required elements as specified in state law, by August 2020, Fresno, Los Angeles, Marin, and Sacramento should review their policies and draft or revise them as necessary. Also by August 2020 these agencies should post their revised policies on their websites in accordance with state law.

- To protect ALPR data to the appropriate standard, Fresno, Los Angeles, Marin, and Sacramento should do the following:
  - By August 2020, identify the types of data in their ALPR systems and, as they review or draft their ALPR policies, ensure that they clarify the types of information their officers may upload into their ALPR systems, such as, but not limited to, information obtained through CLETS.
  - By August 2020, perform an assessment of their ALPR systems' data security features, and make adjustments to their system configurations where necessary to comply with CJIS policy best practices based on that assessment.
- To ensure that the agreements with their cloud vendor offers the strongest possible data protections, by August 2020, Fresno, Marin, and Sacramento should enter into new contracts with Vigilant that contain the contract provisions recommended in CJIS policy.
- To ensure that ALPR images are being shared appropriately, the specific agencies noted should do the following:
  - By April 2020, Fresno, Marin, and Sacramento should review the entities with which they currently share images, determine the appropriateness of this sharing, and take all necessary steps to suspend those sharing relationships deemed inappropriate or unnecessary.
  - As Los Angeles develops its ALPR policy, it should be certain to list the entities with which it will share ALPR images and the process for handling image-sharing requests.
  - By August 2020, Marin and Sacramento should each develop a process for handling ALPR image-sharing requests that includes maintaining records separate from the Vigilant system of when and with whom they share images. The process should verify a requesting agency's law enforcement purpose for obtaining the images and consider the requesting agency's need for the images. The process should be documented in the agency's ALPR policy and/or procedures.
  - By August 2020, Fresno should revise its written procedures for ALPR image-sharing, as necessary, to ensure that it follows those procedures.

- To minimize the privacy risk of retaining ALPR images for long periods of time, Fresno, Los Angeles, Marin, and Sacramento should do the following:

  - By August 2020, review the age of the ALPR images their personnel are searching for and ensure that their retention periods for ALPR images are based on department needs. Each agency should reflect in its ALPR policy the updated retention period and state in its policy that it will reevaluate its retention period at least every two years.

  - Include in their ALPR policies a retention period for data or lists, such as hot lists, used to link persons of interest with license plate images, and create necessary processes to ensure that those data unrelated to ongoing investigations are periodically removed from their ALPR systems.

- To ensure that ALPR system access is limited to agency staff who have a need and a right to use ALPR data, Fresno, Los Angeles, Marin, and Sacramento should do the following:

  - By April 2020, review all user accounts and deactivate accounts for separated employees, inactive users, and others as necessary.

  - Ensure that their ALPR policies specify the staff classifications, ranks, or other designations that may hold ALPR system user accounts and that accounts are granted based on need to know and right to know.

  - By August 2020, develop and implement procedures for granting and managing user accounts that include, but are not limited to, requiring that supervisors must approve accounts for users, providing training to users before granting accounts, suspending users after defined periods of inactivity, and requiring regular refresher training for active users and training for users before reactivating previously inactive accounts. Each agency should also ensure that it has procedures in place to deactivate an account immediately for an account holder who separates from the agency or who no longer needs a user account.

- To enable auditing of user access and user queries of ALPR images, Fresno, Los Angeles, Marin, and Sacramento should do the following:

  - By April 2020, assess the information their ALPR systems capture when users access them to ensure that the systems' logs are complete and accurate and that they form a reasonable basis for conducting necessary, periodic audits.

  - Ensure that their ALPR policies make clear how frequently they will audit their ALPR systems, who will perform those audits, who will review and approve the audit results, and how long they will retain the audit documents. Each agency should have in place by February 2021 an audit plan that describes its audit methodology, including, but not limited to, risk areas that will be audited, sampling, documentation, and resolution of findings.

  - By June 2021, implement their audit plans and complete their first audits.

We conducted this performance audit under the authority vested in the California State Auditor by Government Code 8543 et seq. and in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Respectfully submitted,

Elaine M. Howle

ELAINE M. HOWLE, CPA
California State Auditor

February 13, 2020

Blank page inserted for reproduction purposes only.

Appendix A

Summary of ALPR Survey Responses

The Audit Committee requested that we determine ALPR use among law enforcement agencies statewide. Specifically, the Audit Committee asked us to determine whether agencies use ALPR information, what vendors they use, and whether law enforcement agencies have policies and procedures to govern their use and sharing of ALPR information. We surveyed 391 county sheriffs and municipal police departments statewide. We relied upon information from the California State Sheriffs' Association, the California Police Chiefs Association, and the FBI to obtain assurance that our list of statewide local law enforcement was reasonably comprehensive.

Agencies That Did Not Respond to Our Survey

- Anderson Police Department
- Barstow Police Department
- Del Norte County Sheriff's Office
- Lakeport Police Department
- Lodi Police Department
- Mendocino County Sheriff's Office
- Mount Shasta Police Department
- Oceanside Police Department
- San Francisco Sheriff's Department
- Siskiyou County Sheriff's Department

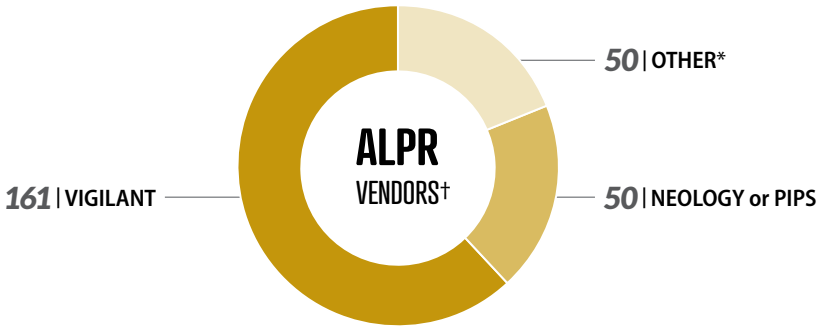
Source: Analysis of survey responses.

We received 381 responses (97 percent) to the 391 surveys we sent. Ten agencies we surveyed did not respond. The text box lists those agencies. A breakdown of the law enforcement agencies' responses to our statewide survey can be found at http://auditor.ca.gov/reports/2019-118/supplemental.html. The discussion here summarizes the survey results.

Summary of Results From Agencies That Reported Using ALPR Systems

In responding to our survey, law enforcement agencies indicated whether they use ALPR systems and, if so, what vendors' systems they use to collect and access ALPR information. Of the agencies that responded, 60 percent, or 230 agencies, reported that they currently operate or access information from ALPR systems. Of those agencies, 96 percent said they have an ALPR usage and privacy policy. Vigilant is the most common vendor for the agencies that reported using ALPR systems. Figure A.1 summarizes which vendors the 230 law enforcement agencies reported that they use. Finally, 9 percent, or 36 of the agencies we surveyed, stated that they are implementing or planning to implement ALPR systems.

Figure A.1
Vigilant Is the ALPR Vendor the Majority of Law Enforcement Agencies Use



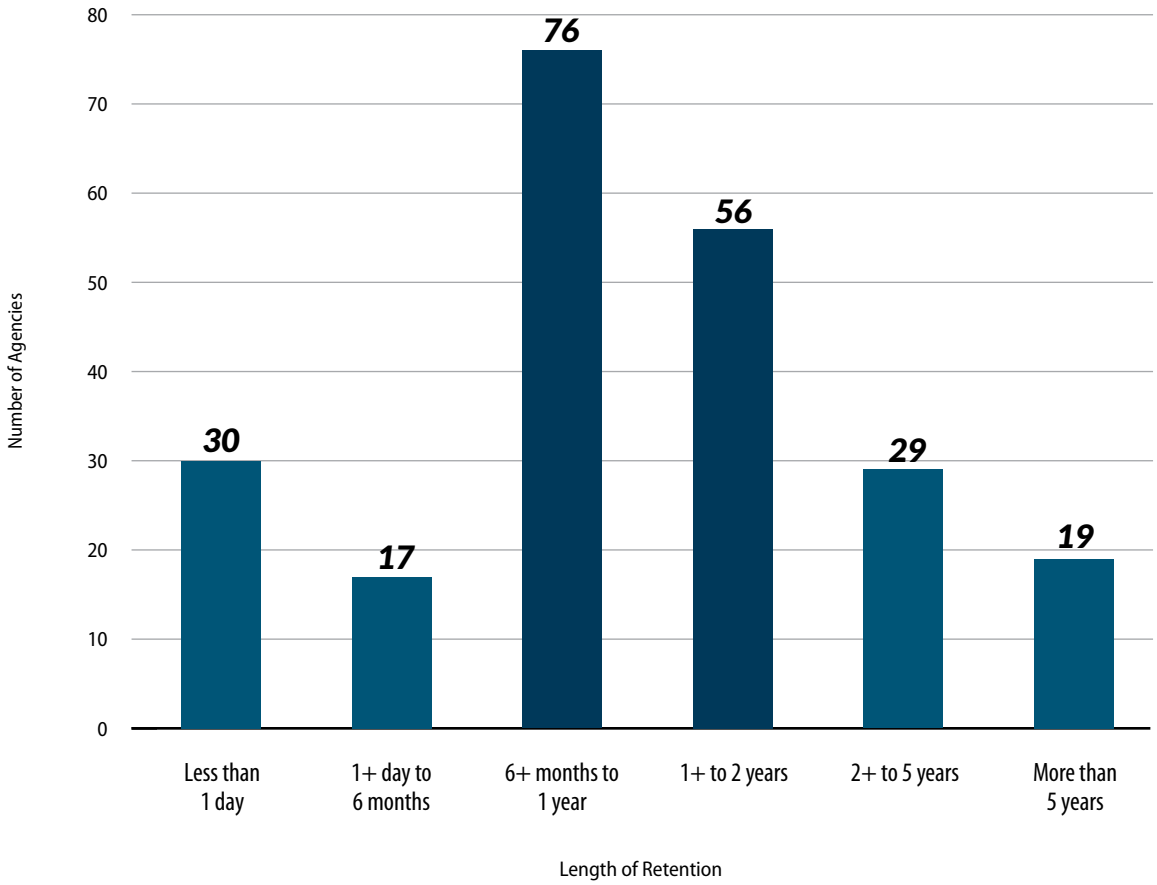
Source: Analysis of survey responses.

* The *Other* category includes vendors such as Genetec, ELSAG, and All Traffic Solutions.

† The total number of ALPR vendors used is greater than the 230 agencies that said they use ALPR systems because some agencies use more than one vendor.

Law enforcement agencies that reported using ALPR systems also answered questions related to their retention and sharing of ALPR information. We asked how long the agencies retain ALPR information not related to ongoing investigations or litigation. As Figure A.2 shows, the retention periods varied, but the majority of law enforcement agencies reported retention periods between six months and two years. Additionally, we asked agencies that operate ALPR systems if they share or sell the information they collect with other law enforcement or public agencies. Seventy-three percent, or 168 agencies that use ALPR systems, reported that they share ALPR images with other law enforcement agencies; only three of those agencies also reported that they share ALPR images with other public agencies that are not law enforcement. None of the agencies we surveyed reported selling images to other law enforcement or public agencies.

Figure A.2
A Majority of Agencies Generally Retain ALPR Information for Between Six Months and Two Years



Source: Analysis of survey responses.

Note: Three responding agencies that use ALPR systems did not indicate a retention period for their information: Bakersfield Police Department, Fountain Valley Police Department, and Pasadena Police Department.

Blank page inserted for reproduction purposes only.

Appendix B

Scope and Methodology

The Audit Committee directed the California State Auditor to conduct an audit of the extent to which local law enforcement agencies are complying with existing law regarding the use of ALPR systems. The analysis the Audit Committee approved contained five objectives. We list the objectives and the methods we used to address them in Table B.

Table B
Audit Objectives and the Methods Used to Address Them

	AUDIT OBJECTIVE	METHOD
1	Review and evaluate the laws, rules, and regulations significant to the audit objectives.	Reviewed relevant state laws, regulations, and other background materials applicable to the use and operation of ALPR systems by local law enforcement.
2	To the extent possible, determine the following for law enforcement agencies statewide: a. Whether they use ALPR information and, if so, what vendors they use to access this information. b. Whether they have policies and procedures in place governing the use and sharing of ALPR information.	• Surveyed 391 county sheriff and municipal police departments statewide. • Obtained and verified a list of statewide local law enforcement agencies, using information from the California State Sheriffs' Association, the California Police Chiefs Association, and the FBI. • Questioned agencies regarding their use of ALPR systems, including whether they use or are planning to use an ALPR system; if they share or sell the ALPR information; if their ALPR storage is CJIS-compliant; which system they use to store, share, or access ALPR information; if they have a usage and privacy policy and post the policy on their website; how long they retain ALPR information; how many department personnel have access to the ALPR data; and how many total personnel their department has. Full questions and a breakdown of the responses are on our website at http://auditor.ca.gov/reports/2019-118/surveys.html. • Created an interactive graphic to display responses by county, assembly district, and senate district at http://auditor.ca.gov/reports/2019-118/supplemental.html. • The survey responses were self-reported, and we did not verify their accuracy.

continued on next page . . .

	AUDIT OBJECTIVE	METHOD
3	Examine the use of ALPRs by the Sacramento County Sheriff's Office and Department of Human Assistance, the Los Angeles Police Department, the Fresno Police Department, and the Marin County Sheriff's Office by performing the following:	
	a. Determine whether they have policies and procedures in place regarding ALPR systems and whether those policies contain the elements state law requires.	• Interviewed the agencies' ALPR administrators. • Obtained and reviewed ALPR policies and procedures and determined whether each agency met state law requirements in this area.
	b. Determine whether they have followed state law regarding all required public notifications related to ALPR systems and information, including required public hearings.	• Interviewed the agencies' public information officers. • Obtained evidence of public notifications and public hearings and determined whether each agency met state requirements in this area.
	c. Determine whether they maintain records of access to ALPR information from both within and outside the agency that includes all required documentation and whether they have ensured that ALPR information has only been used for authorized purposes.	• Interviewed the agencies' ALPR administrators. • Reviewed access records from the agencies' ALPR systems. • Determined whether the agencies conducted any audits or monitoring by interviewing ALPR administrators, staff of internal audit divisions, and executive staff of any oversight entities. We also reviewed relevant policies and procedures. • Reviewed the agencies' internal affairs files for any cases involving ALPR misuse. • Reviewed Justice's and the FBI's audits of the agencies' IT security and the safeguards those audits identified.
	d. Determine whether they have sold, shared, or transferred ALPR information only to other public agencies, except as otherwise permitted by law, and whether they have properly documented these activities.	• Interviewed the agencies' ALPR administrators. • Reviewed reports and records about data sharing from the agencies' ALPR systems. • Reviewed existing memorandums of agreement and understanding for data sharing. • Interviewed executive staff at Vigilant regarding ALPR system functionality and their procedures for verifying the law enforcement purpose of client agencies.
	e. Determine the nature of any contracts with third-party vendors related to ALPR information.	• Interviewed Justice staff responsible for protecting criminal justice information. • Evaluated the agencies' contracts with third-party vendors and determined whether the contracts contained adequate protections for information in the agencies' ALPR systems.
4	Evaluate whether current state law governing ALPR programs can be enhanced to further protect the privacy and civil liberties of California residents.	• Interviewed agencies' investigators and ALPR program administrators. • Reviewed the information in the agencies' ALPR systems and identified the necessary protections for that information. • Obtained the agencies' justifications for their ALPR data retention periods. • Analyzed six months of the agencies' ALPR search records— between late January and September 2019, depending on when we visited the agencies—to determine how often the agencies' personnel searched for older data in their ALPR systems. • Reviewed other states' ALPR data retention laws based on a report from the National Conference of State Legislatures and identified best practices for data retention. • Analyzed laws pertaining to privacy, personal information, and criminal justice information and determined whether changes to current ALPR law would further protect the privacy and civil liberties of California residents.
5	Review and assess any other issues that are significant to the audit.	Reviewed informational material produced by law enforcement agencies, nonprofit organizations, and other entities to identify concerns surrounding privacy and ALPR systems.

Source: Analysis of state law, policies, information, and documentation identified in the table column titled Method.

Assessment of Data Reliability

The U.S. Government Accountability Office, whose standards we are statutorily obligated to follow, requires us to assess the sufficiency and appropriateness of computer-processed information that we use to support our findings, conclusions, and recommendations. In performing this audit, we relied on electronic data files we obtained from Fresno, Los Angeles, Marin, and Sacramento. These files included reports from the agencies' ALPR systems. Because the agencies relied on remote third-party systems to produce the reports, our analysis of these reports was limited to verifying that we had received the information we requested. We did so by reviewing source materials such as user manuals, interviewing vendor staff, and confirming with the agency staff that the number of records in the files we received were correct. We also used electronic lists from the California Police Chiefs Association and the California State Sheriffs' Association to compile a list of statewide police and sheriff departments for our survey. We verified the nature of the data with the associations' staffs, and we also verified record counts by comparing the provided lists with FBI crime-reporting data. We found the data to be sufficiently reliable for our purposes.

Blank page inserted for reproduction purposes only.

XAVIER BECERRA
Attorney General

State of California
DEPARTMENT OF JUSTICE

1300 I STREET
SACRAMENTO, CA 95815-4524
Public: (916) 210-5000
Fax (916) 227-3079
Email: Joe.Dominic@doj.ca.gov

January 28, 2020

Elaine Howle
California State Auditor
621 Capitol Mall, Suite 1200
Sacramento, CA 95814

Re: Draft Audit Report - California State Auditor Report 2019-118; Automated License Plate Readers (ALPR)

Dear Ms. Howle:

The Department of Justice (DOJ) appreciates the opportunity to review the above-mentioned draft audit report. DOJ currently has no program in place to provide policy template and guidance to law enforcement agencies for their ALPR programs. Express authority from the Legislature and funding are needed to implement the recommendations.

If you have any questions or concerns regarding this matter, you may contact me at the telephone number listed above.

Sincerely,

Joe Dominic, Chief
California Justice Information Services Division

For XAVIER BECERRA
Attorney General

cc: Sean McCluskie, Chief Deputy to the Attorney General
Edward Medrano, Chief, Division of Law Enforcement
Chris Prasad, CPA, Director, Office of Program Oversight and Accountability

Blank page inserted for reproduction purposes only.

City of FRESNO
POLICE DEPARTMENT

ANDREW J. HALL
Chief of Police

Mariposa Mall
P.O. Box 1271
Fresno, CA 93715-1271

January 27, 2020

Elaine Howle
California State Auditor
621 Capitol Mall, Suite 1200
Sacramento, CA 95814

Dear Ms. Howle:

On behalf of the men and women of the Fresno Police Department, allow me the opportunity to thank you and your team for the time and effort in completing the Automated License Plate Reader (ALPR) audit at the request of the Joint Legislative Audit Committee. The Fresno Police Department always strives to ensure we maintain excellence and utilize best practices in all facets of service to the community especially concerning personal privacy. Building trust in the community is paramount to our agency as we continue our on-going efforts to be a model community policing agency. We will utilize this audit to ensure those goals are achieved.

The following are the Fresno Police Department's response to the audit recommendations included in the report.

1. *"To ensure that agency ALPR policies contain all of the required elements as specified in state law, by August 2020 Fresno should review their ALPR policies and draft or revise them as necessary. Also by August 2020 post their revised policies on their websites in accordance with state law:*

   The Fresno Police Department has already began reviewing and updating our ALPR policy. In fact, it is nearly complete and will be completed well in advance of the August 2020 recommended timeline.

2. *"To protect ALPR data to the appropriate standard, Fresno should do the following:"*
   a. *By August 2020 identify the types of data in their ALPR systems, and as they review or draft their policies, ensure that they clarify the types of information their officers may upload into their ALPR systems such as, but not limited to information obtained through CLETS."*

   As the audit showed, the Fresno Police Department has not entered personal data into the ALPR system; however we will continue to review data and incorporate into policy the parameters for types of data which can be entered.

   b. *By April 2020 perform an assessment of their ALPR systems data security features, and make adjustments to their system configurations where necessary to comply with CJIS policy best practices based on that assessment.*

The Fresno Police Department IT Manager will assess the ALPR system and ensure it is in compliance with CJIS Security Policy best practices.

3. *"To ensure that the agreement with their cloud vendor offers the strongest possible data protections, by August 2020 Fresno should enter into new contracts with Vigilant that contain the contract provisions recommended in CJIS policy."*

The Fresno Police Department IT Manager will review the Vigilant contract and ensure the contract is updated and in compliance with CJIS Security policy.

4. *To ensure that ALPR images are being shared appropriately:*
    a. *By April 2020 Fresno should review the entities with which they currently share images, determine the appropriateness of this sharing, and take all necessary steps to suspend those sharing relationships deemed inappropriate or unnecessary.*

The Fresno Police Department has suspended most sharing and now only shares images with bordering states.

    b. *By August 2020 Fresno should revise its written procedures for ALPR image sharing, as necessary, to ensure that it follows these procedures.*

The Fresno Police Department will incorporate these changes into the updated policy.

5. To minimize the privacy risk of retaining ALPR images for long periods of time, Fresno should do the following:
    a. *By August 2020 review the age of the ALPR images their personnel are searching for and ensure their retention periods for ALPR images are based on department needs. {REDACTED} reflect in its ALPR policy the updated retention period in its policy the updated retention period and state in its policy that it will reevaluate its retention period at least every two years.*

Based on the results of the audit, the Fresno Police Department will amend our current practice of retaining images for one year to six months which is consistent with the time frame the majority of the searches occur.

    b. *Include in their ALPR policies a retention period for data or lists such as hot lists, used to link persons of interest with license plate images, and create necessary processes to ensure that those data unrelated to ongoing investigations are periodically removed from their ALPR systems.*

The Fresno Police Department will maintain active hot lists for 90 days. If an investigator requires a longer period, approval will be obtained from a commander. This will be incorporated in the revised ALPR policy.

6. To enable monitoring of user access and user queries of ALPR images, Fresno should do the following:
    a. *By April 2020 assess the information their ALPR systems capture when users access them to ensure that the systems' logs are complete and accurate and that they form a reasonable basis for conducting necessary, periodic audits.*

This is already being done and is part of the quarterly audit process.

    b. *Ensure their ALPR policies make clear how frequently they will audit their ALPR systems, who will perform those audits, who will review and approve the audit results, and how long they will retain the audit documents. [REDACTED] have in place by February 2021 an audit plan that describes its audit methodology, including, but not limited to, risk areas that will be audited, sampling, documentation, and resolution of findings.*

A quarterly audit process has been put in place. The audit process, methodology and responsibilities will be included in the updated ALPR policy.

    c. *By June 2021 implement their audit plans and complete their first audits.*

The audit process is already in place and audits were completed for the last two quarters of 2019.

7. To ensure that ALPR access is limited to agency staff who have a right and a need to use ALPR data, Fresno [REDACTED] should do the following:
    a. *By April 2020 review all user accounts and deactivate accounts for separated employees, inactive users, and others as necessary.*

This has been completed. Separated employees are removed upon notification of their separation. The ALPR system automatically deactivates accounts for users who have been inactive for 365 days.

    b. *Ensure that their ALPR policies specify the staff classifications, ranks, or other designations that may hold ALPR system user accounts and that accounts are granted based on need to know and right to know.*

This will be incorporated into the revised ALPR Policy. Access will be granted on a need to know and right to know basis for sworn department members and crime specialists who have investigative responsibility.

    c. *By August 2020 develop and implement procedures for granting and managing user accounts that include, but are not limited to, requiring that a supervisor must approve an account for a user, providing training to users before granting an account, suspending users after defined periods of inactivity, and requiring regular refresher training for active users and training for users before reactivating previously*

inactive accounts. [REDACTED] ensure that it has procedures in place to deactivate accounts immediately for account holders who separate from the agency or who no longer need a user account.

The Fresno Police Department will incorporate supervisor approval for new accounts and minimum training requirements for new users in the revised policy.

Sincerely,

Andrew J. Hall, Chief of Police
Fresno Police Department

AJH: rb

LOS ANGELES POLICE DEPARTMENT

MICHEL MOORE
Chief of Police

ERIC GARCETTI
Mayor

P. O. Box 30158
Los Angeles, Calif. 90030
Telephone: (213) 486-0150
TDD: (877) 275-5273
Ref #: 1.1

February 4, 2020

Elaine Howle*
California State Auditor
621 Capitol Mall, Suite 1200
Sacramento, CA 95814

Dear Ms. Howle:

In response to your draft report titled "Automated License Plate Readers: To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards Over the Data It Collects," I would like to inform you that the Los Angeles Police Department (LAPD) has the utmost respect for individuals' privacy and currently has policies and procedures in place to safeguard personal information stored on the Automated License Plate Reader (ALPR) Systems. Personnel who utilize ALPR data have been through extensive training on accessing and using the data on a right to know and need to know basis. The LAPD continuously reviews all user accounts and deactivates accounts for separated employees, while allowing ALPR access to all active employees who have attended the training. ① ②

Although our dedication to protecting individuals' privacy is covered in our day to day operations and procedures, the Department is currently working on an ALPR policy to ensure that the protection of those rights is also memorialized in our Department Manual. The aforementioned ALPR policy will be completed by April 2020 and posted on the Department website once it is completed, as required by state law. The policy will address the types of information personnel may upload into the ALPR systems, as well as the retention period for the data or lists (i.e., hot lists used to link persons of interest with license plate images). The LAPD will perform an assessment of the systems' data security features and retention periods for ALPR images to evaluate the need for adjustment, prior to publishing of the ALPR policy. Furthermore, the policy will list the entities the Department shares ALPR images with and the process for handling image-sharing requests.

To ensure the ALPR policy is up to date and our ALPR systems are capturing proper information, the Department will perform periodic audits to assess the information the systems capture when accessed by the Department users. Per the recommendations listed in your audit draft report, the Department will have a plan that describes the periodic audits by February 2021 and will complete the first audit by June 2021.

Should you have any questions concerning this matter, please contact Sergeant Monica Tokoro, at (213) 486-0197.

Very truly yours,

MICHEL R. MOORE
Chief of Police

* California State Auditor's comments appear on page 61.

Blank page inserted for reproduction purposes only.

Comments

CALIFORNIA STATE AUDITOR'S COMMENTS ON THE RESPONSE FROM THE LOS ANGELES POLICE DEPARTMENT

To provide clarity and perspective, we are commenting on the response to our audit report from the Los Angeles Police Department. The numbers below correspond with the numbers we have placed in the margin of its response.

Los Angeles is the only one of four agencies we audited that did not have the ALPR policy state law requires. As we describe on page 15, state law requires law enforcement agencies to have written usage and privacy policies and for the policies to include various elements. As we describe on page 17, the program administrator for Los Angeles initially believed that the agency's many IT policies cover the ALPR program, but we identified deficiencies in the policies he shared with us. When we brought those deficiencies to the administrator's attention, he acknowledged the need for Los Angeles to have an ALPR policy. ①

We stand by our conclusion that Los Angeles does not follow best practices for granting users ALPR system access. As we describe on page 33, of the four agencies we reviewed Los Angeles was the most lax in its approach to authorizing user accounts. The protocol its IT division follows is to include its ALPR software on each computer it assigns to staff, regardless of their position. Thus, staff who do not perform functions related to the ALPR system and possibly have not had training, nevertheless have access to the system. Moreover, on page 34 we state that the detective who conducts ALPR training confirmed that Los Angeles has not required training before users can access the ALPR system. ②

Blank page inserted for reproduction purposes only.

COUNTY OF MARIN

OFFICE OF THE
COUNTY COUNSEL

Brian E. Washington
COUNTY COUNSEL

Jack F. Govi
ASSISTANT COUNTY COUNSEL

Renee Giacomini Brewer
CHIEF DEPUTY COUNTY COUNSEL

Patrick M. K. Richardson
Stephen R. Raab
Steven M. Perl
Brian C. Case
Jenna J. Brady
Valorie R. Boughey
Kerry L. Gerchow
Tarisha K. Bal
Deidre K. Smith
Brandon W. Halter
Sarah B. Anker

DEPUTIES

Colleen McGrath
ADMINISTRATIVE SERVICES OFFICER

Marin County Civic Center
3501 Civic Center Drive
Suite 275
San Rafael, CA 94903
415 473 6117 T
415 473 3796 F
415 473 2226 TTY
www.marincounty.org/cl

January 28, 2020

Elaine M. Howle, CPA*
California State Auditor
621 Capitol Mall, Suite 1200
Sacramento, CA 95814

Dear Ms. Howle:

The Marin County Sheriff's Office appreciates the opportunity to respond to your draft report entitled, Automated License Plate Readers: To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards Over the Data It Collects.

The Marin County Sheriff's Office is pleased to note that although your draft report includes recommendations to the Marin County Sheriff's Office regarding its use of automated license plate reader (ALPR) cameras, your audit team did not find any evidence of abuse or misuse of ALPR data by the Marin County Sheriff's Office. (1)

Nevertheless, the Marin County Sheriff's Office is and remains committed to the need for further improvement and as stated in your draft report, will consider your report's recommendations. However, based on some of the redactions in the draft report, it is difficult, at times, to determine which findings and conclusions are in reference to the Marin County Sheriff's Office as opposed to the other confidential law enforcement agencies discussed in your draft report. (2)

Accordingly, in responding to the issues discussed in your draft report with additional details and/or context, the Marin County Sheriff's Office will address sections which may not apply to it because it is unable to distinguish which law enforcement agency is being implicated. (2)

The following is the Marin County Sheriff's Office response:

Recommendation No. 1: Improve their ALPR polices.

Response to Recommendation No. 1: While the Marin County Sheriff's Office agrees that its current policy regarding the ALPR system does not specifically describe a "process for periodic system audits," the Marin County Sheriff's Office's policy does state that user/data query audits would be performed. Moreover, although the audit team contends that the ALPR data collected by the

* California State Auditor's comments begin on page 67.

PG. 2 OF 4

Marin County Sheriff's Office qualifies as personal information, this is not the case. The draft report readily admits that there is no personally identifiable information contained in a license plate capture. Further, the audit team's erroneous belief is based on a free text box in the ALPR system wherein a user *could* enter a person's name in this text box and attach personal information to the images of license plates captured by the ALPR system. However, the Marin County Sheriff's Office does not utilize this free text box and does not enter any other personal information to be associated with the images taken by its ALPR system. In fact, the draft report concedes this fact as it states in regard to the Marin County Sheriff's Office and open text fields, the audit team "did not find personal information in combination with other sensitive information in the six months of search records [it] studied."

Recommendation No. 2: Implement needed ALPR data security.

Response to Recommendation No. 2: As noted in the draft report, the Marin County Sheriff's Office contracts with a third-party vendor Vigilant Solutions (Vigilant) regarding its ALPR system. While the audit team is critical of Vigilant, all access to Vigilant for the Marin County Sheriff's Office is activity logged and auditable as noted in the draft report, even if the user accesses the system via the internet with a personal device, and those logs are reviewed by the Marin County Sheriff's Office ALPR program administrator; all data on Vigilant is stored on secure servers in the United States as recommended by the audit team; and Vigilant only permits credentialed law enforcement officers with a valid Originating Agency Identifier (ORI) number issued by the Criminal Justice Information System (CJIS) Division of the Federal Bureau of Investigation (FBI). Additionally, as part of its services, Vigilant maintains it is compliant with all relevant requirements set forth in the FBI-CJIS Security Policy as recommended by the audit team.

Recommendation No. 3: Update vendor contracts with necessary data safeguards.

Response to Recommendation No. 3: As discussed above, while not explicitly stated in the Marin County Sheriff's Office's contract with Vigilant, Vigilant warrants in its services that the data captured by an agency remains the property of the agency; all data is stored on secure servers in the United States; and it conforms with all relevant requirements set forth in the FBI-CJIS Security Policy.

Recommendation No. 4: Ensure that sharing of ALPR images is done appropriately.

Response to Recommendation No. 4: As discussed above, the Marin County Sheriff's Office has confirmed with Vigilant that it has and continues to verify that it only permits credentialed law enforcement officers with a valid ORI number issued by the CJIS Division of the FBI access to the data on its hosted

PG. 3 OF 4

server. While the audit team was critical of the Marin County Sheriff's Office sharing information with agencies such as the Honolulu Police Department, such cooperation with this particular law enforcement agency was done properly and with consideration as to the multiple matters which have in the past involved both agencies. (6)

As for ICE access, any prior approval by the Marin County Sheriff's Office with Vigilant was before any of the relevant state law went into effect. As noted in the draft report, Vigilant confirmed that the recent viewing of ICE accounts in question were not active and that these inactive agencies were not previously visible to the Marin County Sheriff's Office. (6)

Recommendation No. 5: Evaluate and reestablish data retention policies.

Response to Recommendation No. 5: The Marin County Sheriff's Office's two-year retention policy is based on the statute of limitations for most crimes in the State of California. The audit team states that it would like the Marin County's Sheriff's Office to have a more detailed policy regarding retention based on usefulness of images to investigators and even suggest that the retention of the images should be based on whether the images are for minor crimes versus complex crimes. However, it would be impossible for the Marin County Sheriff's Office to know whether the captured images would be used in a minor criminal case or a major felony case at the time the images were taken or at any time afterwards. Indeed, as noted in the draft report, there is no statute of limitations for the crime of murder. (7)

Recommendation No. 6: Develop and implement procedures for granting and managing user accounts.

Response to Recommendation No. 6: The audit team believes that the Marin County Sheriff's Office should require supervisory approval for all users of its ALPR system. As noted above and in the draft report, at this time the Marin County Sheriff's Office does not believe that this particular requirement is appropriate for the following reasons: there is no personal information associated with the images taken by the Marin County Sheriff's Office; as discussed in the draft report, all users of the ALPR system receive training before they are permitted access to the ALPR system; and the Marin County Sheriff's Office regularly audits the use of the ALPR system. (8)

Recommendation No. 7: Develop and implement ALPR system oversight.

Response to Recommendation No. 7: In the draft report, the audit team identifies an incident in which it claims it brought to the Marin County Sheriff's Office's attention an active account for a resigned employee. However, this is not accurate. The system administrator was notified about deactivating the account on the same day the audit team informed him about this account. However, the (9)

ALPR administrator had deactivated the account *prior* to the audit team discussing this particular account with him. Moreover, the ALPR administrator does not solely rely on a department-wide email notification regarding resigned or terminated employees as discussed in the draft report. In addition to the audits he regularly performs, the ALPR administrator also performs periodic spot checks to verify that active accounts match active employees.

Should you have any questions regarding this response, including any comments and clarifications made herein, please do not hesitate to contact us directly.

Sincerely,

Kerry L. Gerchow
Deputy County Counsel

Comments

CALIFORNIA STATE AUDITOR'S COMMENTS ON THE RESPONSE FROM THE MARIN COUNTY SHERIFF'S OFFICE

To provide clarity and perspective, we are commenting on the response to our audit report from the Marin County Sheriff's Office. The numbers below correspond with the numbers we have placed in the margin of its response.

Marin's response correctly notes that our review of its internal affairs investigations records did not identify evidence of abuse or misuse of ALPR data. However, as we state on page 37, we do not consider this absence as proof that no instances of ALPR misuse occurred. There is the possibility that misuse occurred and went unnoticed and unreported, particularly since Marin does not conduct audits of its ALPR system. (1)

During our exit conference, we specifically informed Marin that we would send it only those portions of the draft report that were relevant to it. The text that we redacted pertains to the other entities that were part of the audit and that we are required by law to keep confidential. Further, during its review of the draft report, Marin did not communicate with us to seek clarification regarding the report content we provided, despite our providing multiple opportunities for it to do so. (2)

Marin is incorrect in stating that we contend that the license plate images Marin collects qualify as personal information. On page 11, we note that a law enforcement agency can enter additional information, such as personal information, into its ALPR system. However, we do not assert that the ALPR image alone contains personal information. (3)

Marin has mischaracterized our finding. In its response, Marin states that we based our conclusion on a free-text box wherein a user could enter an individual's name and attach it to a license plate image. However, as we describe on pages 18 and 19, we based our conclusion on information that users enter into open text fields as part of license plate searches, specifically the fields for case numbers and purpose for the searches. On page 37, we note that Marin requires users to enter both case numbers and reasons for the search before allowing such searches. Although we did not find evidence users had entered personal information in combination with other sensitive information in the six months of search records we studied, the fact that these text fields exist means that users could enter such information during ALPR searches, as we point out on pages 18 and 19. Moreover, Marin's ALPR policy does not prohibit users from entering personal information in combination with other sensitive information in its ALPR system. (4)

5 We disagree with the focus of Marin's response, which implies that the vendor's security controls are a suitable substitute for specific contract safeguards. As we show in Figure 3 on page 22, Marin's contract does not contain any of the safeguards CJIS policy recommends for contracts with cloud vendors. We note on page 21 that CJIS policy states that ambiguous contract terms can lead to controversy over data privacy and ownership rights, whereas a contract that clearly establishes data ownership acts as a foundation for trust that the cloud vendor will protect the privacy of the agency's data.

6 We disagree with Marin's belief that it has managed its image sharing appropriately. Although Marin described in its response the type of information that it could maintain to document its image-sharing decisions, it did not provide such evidence documenting why it made past sharing decisions, and its ALPR policy does not include a process for approving image-sharing requests, as we state on page 26. Moreover, Marin acknowledged in its response the issue we describe on page 26 regarding ICE and the fact that the status of Marin's sharing relationship with ICE was not always visible to Marin. This issue underscores the need for Marin to maintain records regarding sharing decisions.

7 Marin appears to miss the point of our recommendation. As we state on page 29, we concluded that Marin did not establish its retention period based on when it uses the ALPR images it captures. On page 31, we mention minor and complex crimes as examples of ALPR data being used narrowly, such as for the single purpose of locating stolen vehicles, or broadly, such as for investigation of crimes in addition to stolen vehicles. Our recommendation—based on our analysis of Marin's search activity as referenced on page 30—provides a method for Marin to better align how long it retains ALPR data with whether it actually uses the data as they age.

8 The reasons Marin cites in its response for not adopting our recommendation are not valid. Requiring a supervisor to approve a user for an ALPR account is a meaningful step in establishing that user's need to access ALPR data and right to know what the data portray in an effort to avoid the ALPR data being misused. In point 4 above, we describe that the existence of text fields in the ALPR system allows for personal information to be linked to license plate images. Further, we note that Marin has no policy prohibiting its users from entering personal information in its ALPR system. In addition, despite Marin's claim of training all users, we state on page 34 that Marin does not require staff to renew their training when reactivating their user accounts following long periods of not using the ALPR system. Finally, we found that contrary to Marin's assertion, it had not regularly audited its system. As we discuss

on page 37, Marin's ALPR administrator was unaware of the state law requiring audits of ALPR systems, so he had not been conducting them. Despite recent efforts to institute some form of monitoring, as we describe on page 38, the limitations in its approach led us to conclude that Marin does not have sufficient protocols in place to detect the misuse of user accounts.

Marin's assertion is incorrect. As we describe on page 35, we reviewed Marin's processes for disabling the accounts of separated employees. Although Marin's ALPR administrator informed us of his approach for deactivating an account when he receives an all-staff email that an employee is separating from the department, we found such an email dated August 6, 2019, after which one separated employee continued to hold an active account as of October 22, 2019. After we informed the administrator of this employee's continued access, the administrator acknowledged that the account was still active, and we directly observed him deactivating the account. ⑨

Blank page inserted for reproduction purposes only.

Human Assistance
Ann Edwards, Director

County of Sacramento

Branches
Customer Service Operations
Finance and Administration
Community and Program Support

County Veterans Services Office

January 27, 2020

Elaine M. Howle
California State Auditor
621 Capitol Mall, Suite 1200
Sacramento, CA 95814

SUBJECT: License Plate Readers Audit Response

Dear Ms. Howle:

We are writing in response to the draft findings of your report, titled Automated License Plate Readers: To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards Over the Data It Collects.

The Department of Human Assistance (DHA) appreciates the work performed by the California State Auditor. No recommendations were issued in the report, and DHA agrees with the results of the audit.

If you have any questions regarding this matter, please contact Lane Ruddick, Program Integrity Chief, by telephone at (916) 875-1275, or by email at ruddickl@saccounty.net.

Sincerely,

Ann Edwards
Director

Blank page inserted for reproduction purposes only.

SACRAMENTO COUNTY SHERIFF'S OFFICE

Scott R. Jones
Sheriff

January 28, 2020

Elaine M. Howle, CPA*
California State Auditor
621 Capitol Mall, Suite 1200
Sacramento, CA 95814

Dear Ms. Howle:

I am in receipt of the draft report entitled *Automated License Plate Readers: To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards Over the Data It Collects, which* includes recommendations for the Sacramento County Sheriff's Office to revise and improve some of our Automated License Plate Reader program (ALPR) processes.

While I agree with some of your findings, I disagree with some of the characterizations made. ① As the Sheriff of Sacramento County, I take seriously the protection of our citizens, including their personal privacy. Within our role as guardians of the data we collect, my staff works diligently to develop and consistently apply security protocols that maintain the integrity of our systems.

The Summary (Results in Brief) section of the report was clearly written separately or prior to ① the completion of the main body of the report, because it fails to present your teams' actual conclusions. Let me address each point.

Recommendation #1 – Review and revise policies

Before the Audit began, the Sacramento County Sheriff's Office began reviewing and revising policies governing a wide range of service deliverables. Although the Sacramento County Sheriff's Office existing policy contains the majority of the requirements outlined in California Civil Code section 1798.90.51, it does not list the restriction on selling ALPR data. As expressed during the interviews, my staff did say that the restriction on selling data is not listed in the policy because the Sacramento Sheriff's Office does not sell any data. The lack of specifically addressing this fact in the ALPR policy is an oversight.

* California State Auditor's comments begin on page 77.

Elaine M. Howle, CPA
January 28, 2020
Page 2

Recommendation #2 – Identify types of data and perform a security assessment

As you learned during the audit, the Sacramento County Sheriff's Office began reorganizing ALPR related security over two years ago. The initial step of this process was securing funding to hire a fulltime Information Technology Analyst in hopes of increasing program administration because this employee's primary job will be the continuous development of ALPR related security protocols that either meet or exceed these recommendations.

Recommendation #3 – Ensure the vendor offers the strongest possible data protections

The Sacramento County Sheriff's Office completed extensive research in the use of cloud storage systems and CJIS security. I am aware your team received the latest contract between the Sacramento County Sheriff's Office and Vigilant Solutions and the Vigilant CJIS Security Policy Guide. Both the contract and comprehensive policy provide a thorough explanation regarding compliance including agreeing to participate in any Technical Security Compliance Audit performed by the FBI-CJIS Division. ②

Recommendation #4 – Develop a process for handling ALPR image-sharing requests

③ Although the existing policy does provide language on how sharing data can occur, the Sacramento County Sheriff's Office began developing a ticketing system for handling various technology requests over four years ago. As such, the natural progression was to utilize the same request, approval, and record retention system used by the entire organization.

Recommendation #5 – Review the retention periods of ALPR images and data

The Sacramento County Sheriff's Office is continually reviewing data retention practices. Although, a simple review of searches provides a small subset of activity, the success of an ALPR program could only come from tracking and identifying which cases provided leads or convictions of data. During the audit, my understanding is your team was told this very fact. As ④ the agency prepares to transition to a new report writing system, I request our crime analysts to conduct a multi-year study that will provide a realistic view of how long ALPR images provide usefulness in the criminal justice system.

Recommendation #6 – Enable monitoring of user access and user queries of ALPR images

Throughout the audit your team requested a substantial number of reports and logs showing when accounts were activated, deactivated, or changes occurred. The ability to provide these reports demonstrated the robust nature of the logging system. Although your team learned the

Elaine M. Howle, CPA
January 28, 2020
Page 3

Sacramento County Sheriff's Office has no reported incidents of ALPR misuse, I have directed my program administrator to make certain fields mandatory to ensure proper documentation of usage. With the addition of a dedicated IT Analyst, the expansion of audits already occurring will surely continue.

Recommendation #7 – Ensure that ALPR access is limited to agency staff who have a right and a need to know

Not only is this recommendation listed in the Sacramento County Sheriff's Office policy, it is the way the organization operates with all data systems. As this directly relates to ALPR, only 561 employees, out of a department of 2,170, have access to the system. While I understand your position that a supervisor should approve each account, there were over 5,880 personnel moves during 2019. The Sacramento County Sheriff's Office uses Role Based Access Controls. Rather than rely solely on a supervisor to approve a request, the application of Role Based Access Control is how the Security Operations unit of the Sacramento Sheriff's Office processes access to this and all other law enforcement data systems. Role Based Access Controls are addressed by the National Institute of Standards and Technology as a best practice. (5)

In Conclusion

In the end, we are not opposed to implementing many of your recommendations and in fact, are already in the process of doing so. Throughout the process, which was long and took many staff hours, we made every effort to cooperate with the auditor's requests for information and tried to anticipate the types of problems they would find while trying to understand the actual uses and practices within the ALPR program.

During interviews and based on some of the requests, we felt concern that there was a bias toward a particular outcome, intended or otherwise. (6) Because this report contains many redacted sections, there is still some concern about what has not been shown to us. Nonetheless, we await your full findings about Sacramento and the other agencies covered in this report. (7)

Very truly yours,

Scott Jones

SCOTT R. JONES, SHERIFF

Blank page inserted for reproduction purposes only.

Comments

CALIFORNIA STATE AUDITOR'S COMMENTS ON THE RESPONSE FROM THE SACRAMENTO COUNTY SHERIFF'S OFFICE

To provide clarity and perspective, we are commenting on the response to our audit report from the Sacramento County Sheriff's Office. The numbers below correspond with the numbers we have placed in the margin of its response.

We stand by the language we use to describe Sacramento's ALPR program. Our report provides appropriate context and sufficient evidence to support our findings. Further, the Results in Brief section of the report serves as a summary of the report as a whole and as such it represents the overall conclusions for this report. The details of our findings and conclusions are included in the Audit Results section of the report. ①

We disagree with Sacramento's contention that the department's current contract is thorough. On pages 22 and 23, we acknowledge that Sacramento updated its contract with Vigilant in September 2019. In reviewing that latest version, we determined that it is missing some of the best practices outlined in CJIS policy, as we show in Figure 3 on page 22. On page 21, we note that CJIS policy states that a contract that clearly establishes data ownership acts as a foundation for trust that the cloud vendor will protect the privacy of the agency's data. ②

Sacramento's response implies that a process for approving image-sharing requests and maintaining records outside of the Vigilant system was already in place. However, although Sacramento states that it began developing a ticketing system for handling technology requests more than four years ago, as we discuss on page 26, Sacramento could not provide any evidence of records outside of the Vigilant user interface demonstrating when or why it agreed to share with particular entities. As we further point out on page 26, Sacramento's ALPR policy currently does not include a process for approving sharing requests. ③

Sacramento's proposed study of ALPR images may benefit its ALPR program. Our analysis of the search records from the agencies we reviewed—summarized on page 30 and in Table 2—presents one method of identifying the age of the data personnel are using. We point out on page 31 that the agencies' existing ALPR systems provide the ability to conduct such an analysis. Nevertheless, our recommendation does not preclude the type of analysis Sacramento describes in its response. ④

⑤ We stand by our recommendation that Sacramento should have a policy that clearly states the staff classifications, ranks, or other designations that may hold ALPR system user accounts and that accounts are granted based on a need to know and a right to know. As we state on page 32, each ALPR administrator, including Sacramento's, stressed the concept of "need to know, right to know." Assigning an individual an ALPR account based strictly on his or her classification or role—the practice Sacramento follows—does not ensure that an individual has a need to know because of their specific assigned work.

⑥ Sacramento's concern about bias is unfounded. To meet generally accepted government auditing standards, which my office is obligated to comply with, we have and follow policies and procedures for all audits to ensure that we identify and rectify any threats to our independence, including bias. Moreover, we follow quality control procedures on every audit that ensure that we have sufficient and appropriate evidence to support our findings and conclusions.

⑦ Sacramento received draft text that was relevant to our findings about it. State law requires us to keep confidential information about an unpublished audit. Consequently, we cannot share with one agency information about another. Sacramento received a draft audit report with redacted information regarding other agencies as necessary to maintain confidentiality. During our exit conference, we stressed that staff should contact us with questions they might have about the draft report during the formal review period; Sacramento did not contact us. We also contacted Sacramento's ALPR administrator during the formal review period to inquire about questions staff may have, and he did not return our call.

STATE OF NEW JERSEY
DEPARTMENT OF LAW AND PUBLIC SAFETY
OFFICE OF THE ATTORNEY GENERAL

FY21 AMERICAN RESCUE PLAN (ARP) ACT – CORONAVIRUS STATE FISCAL RECOVERY FUND (CSFRF)

AUTOMATED LICENSE PLATE READER INITAITIVE

PROGRAM ADMINISTRATION AND GUIDELINES

STATE OF NEW JERSEY
FY21 AMERICAN RESCUE PLAN ACT CSFRF
AUTOMATED LICENSE PLATE READER INITAITIVE
PROGRAM ADMINISTRATION AND GUIDELINES

I. ADMINISTRATION

This document has been compiled to assist in the application, program development, and implementation processes, as well as the reporting and compliance requirements, of the FY21 ARP CSFRF Automated License Plate Reader Initiative.

The State of New Jersey, Department of Law & Public Safety, Office of the Attorney General (OAG), Division of Criminal Justice (DCJ) received funds from the FY21 ARP CSFRF to administer the Automated License Plate Reader Initiative. A total of $9,750,000 will be awarded to New Jersey law enforcement agencies for use by November 30, 2024.

The goal is to use this technology to not only investigate the increase of stolen cars, but to assist in investigating their connections to the increase in violent crime, including gun violence. Intelligence gathered through the use of this technology will assist law enforcement in identifying suspects, improving solve rates of theft offenses, identifying patterns and criminal enterprises, building more sophisticated cases to deter and prosecute organized criminal activity, and will assist in implementing prevention strategies and operations

Under the ARP CSFRF License Plate Reader Initiative, law enforcement agencies with jurisdiction in the State of New Jersey are eligible to apply for grant funding for the investment in new, and expansion of existing, technology and software system integration of ALPRs. Specifically, funding would cover the cost of purchasing or enhancing ALPR units for law enforcement agencies across New Jersey, as well as initial software, storage, and maintenance for 5 years.

It is anticipated that ALPRs will be installed in fixed locations on the New Jersey Turnpike, Parkway, Atlantic City Expressway, I-195, US Highway 1 and 9, and Routes 21, 22, 78, 80, 280, and 287; in addition to other major highways. Due to these roadways being within the primary investigative jurisdiction of NJSP, $5,000,000 of the grant funds will be allocated to the NJSP to establish this statewide network. The remaining $4,750,000 will be awarded, via a competitive process, to eligible law enforcement agencies for the purchase, installation, and expansion of additional units and systems, in strategic locations throughout the communities they serve. Grant funding will be allocated to both installation at strategic locations, as well as mobile units. Mobile units can be used where there is the greatest need at any given time.

The OAG/DCJ will award, administer, and monitor awards made under the ARP CSFRF ALPR Initiative. Staff from OAG/DCJ will be available to provide technical assistance during the award process and award period.

Funds will be awarded on a competitive basis, supported by statistical data, and awarded pursuant to the quality of the application submitted and the pending availability of funds. The number of awards available and the funding amount of each award will depend upon the number of applications received and the funding amounts requested by each applicant. Funding decisions will be made to ensure the broadest and deepest level of service coverage practicable, taking into account the type of services to be delivered, the desired outcomes, and the geographical location of the project in comparison with crime statistics and data.

The funding period is December 1, 2022 through November 30, 2024; extensions will not be granted. All grant funding must be obligated by November 30, 2024.

All inquiries concerning the grant award process should be addressed to:

Office of the Attorney General
Grant Operations
Phone: 609-376-2445
E-mail address: ALPRGrant@njdcj.org

II. APPLICATION AND AWARD REQUIREMENTS

A. PARTICIPATION and SUBMISSION

Any New Jersey law enforcement agency wishing to participate in the ARP CSFRF Automated License Plate Reader Initiative must complete an application package and submit via e-mail to ALPRGrant@njdcj.org, no later than **11:59pm October 15, 2022**. Late or incomplete applications will **not** be considered for funding.

B. GRANT APPLICATION

Applicants must complete and return the following:

1. Applicant Information Form
2. Application Authorization
3. Program Application Narrative
4. Project Work Plan
5. Budget Detail Worksheet and Narrative
6. New Jersey Single Audit Requirements Certification
7. Federal Single Audit Requirements Certification
8. Proof of Federal Single Audit
9. DLPS Debarred and Suspended Certification
10. Assurances

C. GRANT AWARD

Recipient will be notified of awards on or about November 30, 2022. Award packages will be sent out upon notification of award.

Recipients must complete and return the following:

1. Award Contract
2. Resolution & Certification
3. General and Special Conditions

III. PROGRAM GUIDELINES

The Applicant agrees to adhere to the following guidelines. Failure to do so may result in suspension or termination of a grant award.

- Funding is to be used for purchasing or enhancing ALPR units for law enforcement agencies across New Jersey, as well as initial software, storage, and maintenance for 5 years.
- New Jersey law enforcement recipients will be diligent in communicating with community members to gauge whether changes are needed in coverage area or any other issues related to the implemented technology. Effectiveness of the technology will be primarily driven by any change in data related to violent crime in the various cities, and from feedback from community stakeholders. It will be important to analyze whether the technology is a key tool in gun violence prevention.
- For purposes of insuring compliance with interagency compatibility, all technology and software acquisitions purchased under the grant will require preapproval by the New Jersey State Police. Questions about compatibility can be directed to ALPR@NJSP.ORG.
- Award recipients must be willing to participate in data studies and violence suppression pilot studies being conducted by the DPLS if such participation is requested

IV. APPLICATION AUTHORIZATION

The submission of any grant application requires the signature of the applicant's Authorized Official (see Application Authorization Form) indicating that the application is authorized by the agency or unit of government. The signature of the Authorized Official indicates that the information provided within the application is truthful, accurate, and complete; that the applicant intends to comply with all requirements regarding the use of grant funds; and the applicant will use the grant funds to carry out the project as described in the application.

The Authorized Official also acknowledges that they are responsible for authorizing expenditures and disbursing grant funds. The Applicant certifies that all grant funds will be used exclusively for the purposes specified in the grant award; and it will pay for all costs in excess of the grant award.

V. PROGRAM APPLICATION NARRATIVE

The following scored components must be included in your Program Narrative.

1. Agency Background, Mission, Experience and Capability (10 Points)
Describe in detail the agency's mission, background, and experience as it relates to the purpose and objectives of the proposed project. Explain the agency's knowledge and capability to carry out the project, based on demonstrated experience.

2. Problem Statement/Needs Assessment (25 Points)
Identify the specific problem(s), target population, and geographic area that the proposed project will address. Describe the needs and characteristics of the target population; local needs and conditions; describe existing services and identify gaps and/or barriers in services. Include current statistics and relevant crime data to substantiate the need. Applicants must provide statistics that demonstrate a rise in violenct crime, including gun violence, since the start of the Coronavirus Pandemic.

3. Goals, Objectives and Implementation; Project Work Plan (30 Points)
Specify a clear, realistic goal for the proposed project. Identify objectives that are concise, measurable, and directly relate to the goal, problem statement/needs assessment, and target population. Describe in detail the project's approach or strategy for attaining each objective. Include a project work plan (template to be provided) that specifies each objective along with the major activities, responsible staff, and feasible time frames for each objective and activity.

4. Key Project Staff (10 Points)
Identify all project management and staff. Describe how personnel are uniquely qualified to manage and implement the project.

5. Data Collection/Performance Measures/Evaluation (10 points)
Provide a description of how you will collect data, measure performance, and complete an overall evaluation of the project.

6. Budget Detail and Narrative (15 points)
Applicants must provide an itemized list of costs and a narrative explanation as to why those costs are necessary to the success of the project. Costs must be specific and tied to the project objectives.

VI. BUDGET DETAIL WORKSHEET

Applicant must list all requested budget items on the Budget Detail Worksheet. Costs must be specific and tied to the project objectives. A budget narrative justifying proposed expenditures is also required. The budget narrative should explain why the costs are necessary for the success of the project.

A. Budget Categories:

1. SALARIES

List each position by title and name of employee, if available. Show the annual salary rate and the percentage of time to be devoted to the project. Compensation paid for employees engaged in grant activities must be consistent with that paid for similar work within the applicant organization, and qualifications must be substantiated in the individual's resume. Include a description of the responsibilities and duties of each position in relationship to fulfilling the project goals and objectives.

2. FRINGE BENEFITS

Fringe benefits should be based on actual known costs or an approved negotiated rate. Attach a copy of the fringe benefit policy. Fringe benefits are for the personnel listed in the personnel section of the budget and only for the percentage of time devoted to the project. Fringe benefits on overtime hours are limited to FICA, Workman's Compensation and Unemployment Compensation.

If salaries are being reflected in the budget as a cost of the project, the corresponding fringe should also be included.

3. TRAVEL

Itemize travel expenses of staff personnel by purpose (e.g., staff to training, travel to meetings). Describe the purpose of each travel expenditure in reference to the project objectives. Identify the location of travel, if known; or if unknown, indicate "location to be determined."

Travel costs are allowable if permitted under the current State Travel Circular, 20-04-OMB, as amended, which is located at the following website:
https://www.nj.gov/infobank/circular/
Mileage reimbursement cannot be charged in excess of the New Jersey State maximum of $.47 per mile, per State Treasury Circular Letter, Automobile Mileage Reimbursement Rate, 23-02-OMB.

4. EQUIPMENT

List non-expendable items that are purchased (Note: Organization's own

capitalization policy for classification of equipment should be used.) Expendable items, with a cost less than $1,000, should be included in the "Supplies" category. Applicants should analyze the cost benefits of purchasing versus leasing equipment, especially high cost items and those subject to rapid technological advances. Rented or leased equipment costs should be listed in the "Contractual" category. Explain how the equipment is necessary for the success of the project, and describe the procurement methods to be used.

OAG may approve the purchase of equipment deemed appropriate and essential to the successful operation of projects. Requests for equipment should contain adequate cost specifications, including equipment type, quantity and estimated costs. Specific brand names should be excluded.

Equipment purchased and used commonly for two or more programs should be appropriately divided among each activity. Equipment that has already been purchased and charged to other activities of the organization is not an allowable expense to the award.

5. SUPPLIES

List items by type (office supplies, postage, training materials, copying paper, and expendable equipment items costing less than $1,000, such as books, hand held tape recorders) and show the basis for the computation, Generally, supplies include any materials that are expendable or consumed during the course of the project.

6. CONSULTANTS/CONTRACTS/SUBAWARDS

Provide a description of the product or service to be procured by contract and estimate of the cost. Applicants are encouraged to promote free and open competition in awarding contracts/subawards.

If the application includes a subrecipient(s) to assist in providing services outlined in the scope of work, during the contract award process, special conditions will be added to acknowledge your compliance with the requirements of a pass-through agency for engaging services of a subrecipient agency.

Consultant fees: For each consultant enter the name, if known, service to be provided, hourly or daily fee (8-hour day), and estimated time on the project.

Consultant expenses: List all expenses to be paid from the grant to the individual consultants in addition to their fees (i.e. travel, meals, lodging, etc.). This includes travel expenses for anyone who is not an employee of the applicant such as participants, volunteers, partners, etc.

7. OTHER COSTS

List items by major type and the basis of the computation. For example, provide the square footage and the cost per square foot for rent or provide a monthly rental cost and how many months to rent (rent/lease agreement must be submitted). Only

the cost of facilities used for the project activities are permissible, such as office space, maintenance costs, landlines, and utilities.

VII. RESOLUTION

Applicants must return a certified Resolution with their Award Package.

The Resolution must contain all data requirements listed on the Required Resolution & Certification Checklist which is provided as a reference document in the Award Package.

VIII. LEGAL COMPLIANCE

Applicants and their contractors are required to comply with the New Jersey Law Against Discrimination, N.J.S.A. 10:5-1 et seq. Applicants are expected to comply with all applicable New Jersey regulations, policies, and guidelines.

IX. DEBARMENT

Applicants and their subcontractors should not obtain goods and services from other agencies which are debarred, suspended or disqualified from doing business with the State of New Jersey.

Applicants are also expected to comply with state Executive Order No. 34 (March 17, 1976), and state circular letter OMB 93-13-GSA regarding debarments, suspensions, and disqualifications. The State Department of Treasury has an on-line, searchable database of those individuals, corporations, and agencies, who are debarred from conducting business with the State of New Jersey: http://www.state.nj.us/treasury/revenue/debarment/index.shtml. In the performance of any grant, recipients cannot conduct business with ineligible firms or individuals who are considered debarred, suspended, or disqualified.

X. NEW JERSEY PENALTIES FOR CORRUPTION OF PUBLIC RESOURCES

While enacting ethics and government corruption reforms, the New Jersey Legislature enacted Public Law 2007, Chapter 158, which makes knowingly misusing public resources for an unauthorized purpose a crime. N.J.S.A. 2C:27-12. Under the Crime of Corruption of Public Resources, an individual commits a crime if (1) the public resource is subject to an obligation to be used to perform or facilitate the performance of a governmental function or public service, (2) a person knowingly uses a public resource for an unauthorized purpose, or (3) a person makes a material representation that is false to a government agency . . . to obtain or retain a public resource, or with the purpose to mislead or deceive any person as to the use or disposition of a public resource. Id. The Legislature defines a public resource as including grants awarded by the

government. Id. Convictions under this act could result in a 20-year prison term and $200,000 fine. Id. The Legislature also enhanced public corruption penalties under the Public Corruption Profiteering Penalty Act, N.J.S.A. 2C:30-8, which subjects individuals convicted under public corruption laws, including N.J.S.A. 2C:27-12, to fines up to $500,000. Under N.J.S.A. 2A:32C-3, a person shall also be subject to civil penalty and treble damages for making false claims under New Jersey's False Claims Act.

XI. RECIPIENT OFFICIAL FILE

Recipients are required to maintain a master file for grant documents. The following documents must be available for on-site review by OAG program monitors and auditors:

A. Copy of approved application and award package for the grant including: Applicant Information Form; Application Authorization; Program Narrative; Budget Detail Worksheet; Award Letter; Grant Award Contract; General and Special Conditions; the Resolution; and related written approvals from OAG.

B. Copies of all Requests for Reimbursements.

C. Banking Information: Cash verification, receipts documentation, check register, canceled checks, and bank statements. (if applicable)

D. Copies of all Grant Adjustment requests and approvals.

XII. REPORTING PROCEDURES

A. PROGRAMMATIC REPORTS

Recipients are required to submit quarterly programmatic progress reports to OAG describing project activities for the duration of the award period. Reports are to be submitted to OAG within fifteen (15) calendar days of the end the quarter. Recipients will receive reporting forms with their copy of the executed contract/award document.

B. FINANCIAL REPORTS

Recipients are required to submit financial expenditure reports, or Detailed Cost Statements (DCS), comparing actual expenditures with the OAG Approved Project Budget.

Recipients are required to submit quarterly DCS's. DCS reports must be submitted to your analyst at OAG, via e-mails, within fifteen (15) calendar days of the end of each quarter. The DCS for the last quarter shall be marked as final. For each funding request, a separate State of New Jersey Payment Voucher must be submitted.

1. SOURCE DOCUMENTATION REQUIREMENT

All costs charged to state grant awards must be adequately documented. All recipients must provide supporting source documentation (e.g. invoices, hotel receipts, timesheets, payroll records, purchase orders) with their reimbursement requests. Recipients should be ensuring that their costs are allowable, mathematically accurate and correlate to the source documentation provided. OAG grant staff will review all recipient source documentation prior to approving reimbursement requests. Costs lacking sufficient support may not be reimbursed.

XIII. BUDGET REVISION AND MODIFICATION

The grant budget is the approved financial plan to carry out the purpose of the grant. This plan is the financial representation of the project as approved during the grant application and award process.

Recipients are required to report deviations from the approved budget and receive prior written approvals for budget revisions and modifications in excess of one (1) percent of the total award amount. To request a budget revision, recipients are required to submit a written explanation (Justification Letter) and an OAG Grant Adjustment Request Form (GARF).

XIV. AUDIT REQUIREMENTS

The Recipient must comply with audit requirements located in the State Treasury Department, State Circular, Single Audit Policy for Recipients of Federal Grants, State Grants and State Aid, 15-08- OMB, 2 CFR Part 200, Subpart F, Audit Requirements (2 C.F.R. § 200.500, et seq.), and the Government Accountability Office's Generally Accepted Government Auditing Standards (also known as the Yellow Book).

1. Applicants that expend Federal and/or State financial assistance of $100,000 or more, but less than $750,000 of Federal or State financial assistance during their fiscal year (including federal pass-through funds), must have either:

    a. A financial statement audit performed in accordance with Government Auditing Standards (Yellow Book); or
    b. A program specific audit performed in accordance with 2 C.F.R. § 200.500, et seq., and state policy.

2. For applicants that expend Federal or State financial assistance, (including funds received from the Federal Government or federal funds passed through state agencies) of $750,000 or more during their fiscal year must have:

    a. A single audit performed; or

b. A program specific audit performed in accordance with 2 C.F.R. § 200.500, et seq., and state policy.

3. For applicants receiving less than $100,000 of State and/or Federal financial assistance, no audit is required.

The recipient must maintain a bookkeeping system, records, and files to account for all monies spent implementing the project. While a preferred system is not specified, recipients are expected to conform to accepted accounting standards.

XV. MONITORING OF PROGRAM PERFORMANCE

A. The recipient must assure that performance goals are being achieved.

B. The recipient shall inform OAG of the following types of conditions which affect program objectives and performance as soon as they become known:

Problems, delays, or adverse conditions which will materially impair the ability to attain program objectives, prevent meeting time schedules and goals, or preclude the attainment of project work units by established time periods. This disclosure shall be accompanied by a statement of the action taken, or contemplated, and any OAG assistance required to resolve the situation.

C. OAG may, at its discretion, make site visits to:

1. Review program accomplishments and management control systems.
2. Provide such technical assistance as may be required.
3. Perform fiscal reviews to ensure grant funds are being properly expended in a timely manner.

OAG may also request documents related to the above independent of a site visit. In all cases, Applicant is obligated to comply with requests associated with site visits or document production.

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

flock safety

Falcon Flex™

Location-flexible license plate recognition camera designed for fast, easy deployment



Leverage the same Vehicle Fingerprint ™ technology available on Flock Safety's stationary LPR with the Falcon Flex, an infrastructure-free, location-flexible license plate reader camera. Simple, mobile installation makes this vehicle detection device ideal for your ever-changing investigative needs. Less time to install means faster leads and increased case clearance.



Evidence Capture Simplified

Combine the power of Vehicle Fingerprint recognition with lightweight, adaptable mounting options, and a complementary LTE service is ideal for temporary installation virtually anywhere.

- 1 Falcon License Plate Reader Camera
- 1 Portable mount with varying sized band clamps
- 1 Charger for internal battery
- Unlimited LTE data service + software licenses

Smarter Reads for Actionable Leads

Not every vehicle has a plate. Search by license plates and unique vehicle characteristics including:

- Build type
- Make
- Color
- License plate state
- Missing and covered plates
- Bumper stickers
- Decals
- Roof racks
- & more



Capture More. Recharge Less.

The Falcon Flex camera captures 30,000 license plates and Vehicle Fingerprint attributes of vehicles traveling up to 100 MPH at a maximum distance of 90 feet on a single battery charge.

Activate From the Palm of Your Hand

On-site installation is made quick and easy with the mobile installation app for all your Android and iOS devices, including a DIY installation walkthrough and QR reader for device linking.





Sophisticated Software Outsmarts Crime

Like all Flock Safety detection devices, the Falcon Flex license plate reader camera integrates with Flock Safety's suite of software solutions. With unlimited user licenses, every member of your agency can conduct complex searches, receive Hot List alerts, access 1B+ license place reads each month via our nationwide network of footage sharing and more.

Trustworthy technology that delivers

30K

Plate reads on a single battery charge

120

Stolen plate and vehicle hits every hour

30%

More accurate than legacy ALPR



Camera Specifications

DESIGN
Dimensions: 8.75" x 3"
Weight: 3 lbs
IP65 Waterproof

POWER
14Ah Battery - Rechargeable

DATA
16GB local storage, ~2 weeks

MOTION
Passive Infrared Motion Detection

CONNECTIVITY
Embedded Cellular LTE Connection
Cellular service provider depends on area

PRODUCTION
Designed & manufactured in the U.S.

NIGHT VISION
850nm Custom IR Array

CLOUD STORAGE
30 days storage (Amazon Web Services)
Accessible via secure website
Images can be downloaded and stored by department

Camera Performance

MOTION
NCIC, AMBER Alert & Custom Notifications Average of 10-15 seconds Includes time, location, plate, and vehicle image Includes state-specific alerts based on image

PROCESSING POWER
1.4GHz
64-bit quad-core CPU

IMAGE CAPTURE
Up to 100 ft from vehicles
Up to 2 lanes of traffic per camera
Date and time with camera location
Plate (state, partial, paper, and none)
Vehicle details (Make, type, color, etc.)



Pricing

$3,000/camera per year

Field Technician maintenance is not included; If a camera is lost, stolen, or damaged, a new device can be purchased discounted price of $1500.

flock safety

Law Enforcement



YOUR PARTNER IN ELIMINATING CRIME

Flock Safety provides 1000+ law enforcement agencies in over 2000 cities a scalable solution for public safety that reduces crime by up to 60%. Spend less time chasing investigative leads; leverage Flock Safety's automatic license plate recognition (ALPR) and Vehicle Fingerprint™ technology to get actionable, objective evidence that drives results in your community for less than the cost of hiring an additional officer.

ALPR CAMERAS THAT GO ANYWHERE

Our devices are infrastructure-free with solar power and LTE connectivity, so we can install them quickly where they make the most impact on crime.

CAPTURE MORE THAN LICENSE PLATES

Search footage with Vehicle Fingerprint™ technology. Access vehicle type, make, color, license plate state, missing / covered plates, and other unique features like bumper stickers, decals, and roof racks.

MULTIPLY YOUR FORCE WITH LESS

$2,500 per camera/year includes hardware, software, solar power, data, cloud storage, ongoing maintenance, and access to 1B+ plate reads/month.*

PARTNER WITH YOUR COMMUNITY

Thousands of communities use privately-funded Flock Safety cameras nationwide. This means law enforcement has access to more footage without the additional cost.

INTEGRATED AUDIO DETECTION

Uncover more than shell casings; get from "shots fired" to a suspect vehicle in real-time with the Raven™ audio detection device, an accessory for your ALPR that identifies crimes in progress before 911 is called.

1000+
Agency Re ationships Nationwide

120
Hot List Notifications Per Hour

1B+
License P ate Reads Per Month

2000+
Cities with Private Cameras



Flock Safety's public safety operating system includes fixed license plate reading cameras and software for unlimited users to access footage and receive Hot List notifications.

Learn more at flocksafety.com/lawenforcement

*One-t me $350 mp ementat on fee

1462

Increase Case Clearance for Your Agency with Flock OS



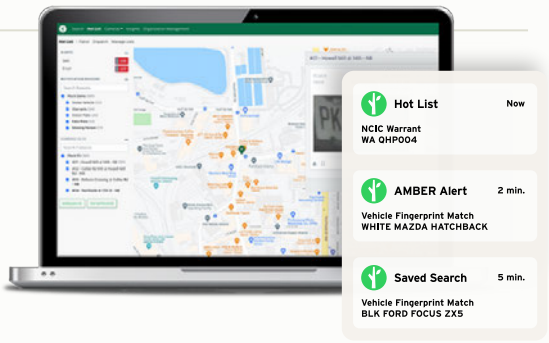
1 DETECT OBJECTIVE EVIDENCE 24/7

Scale public safety without growing your force or exceeding your budget. Instead of knocking on doors after a crime occurs, proactively deploy ALPR cameras or transform existing IP cameras into cameras that see like a detective 24/7 without overtime pay.



2 DECODE FOOTAGE TO UNCOVER LEADS

Our software identifies body type, make, color, license plate (partial, missing, or covered plates), temporary plates, license plate state, and unique features like decals, bumper stickers, and accessories that create a traceable Vehicle Fingerprint.



3 DELIVER ACTIONABLE DATA TO YOUR AGENCY

Give Dispatch a birds-eye view of your jurisdiction and empower your Patrol Officers to be more effective in the field with real-time notifications related to active investigations.

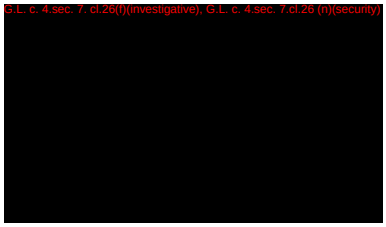
> This technology provides officers the investigative leads necessary to go after suspects immediately, which is great for morale.
>
> Sgt. Adam Senf, Vacaville, CA

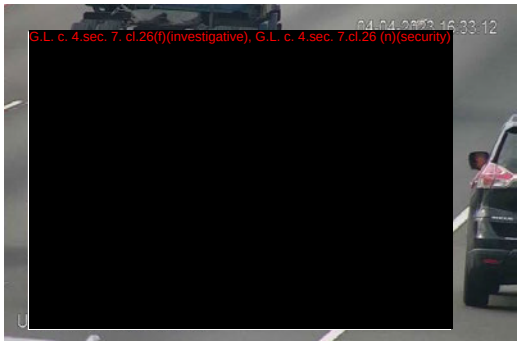
95%

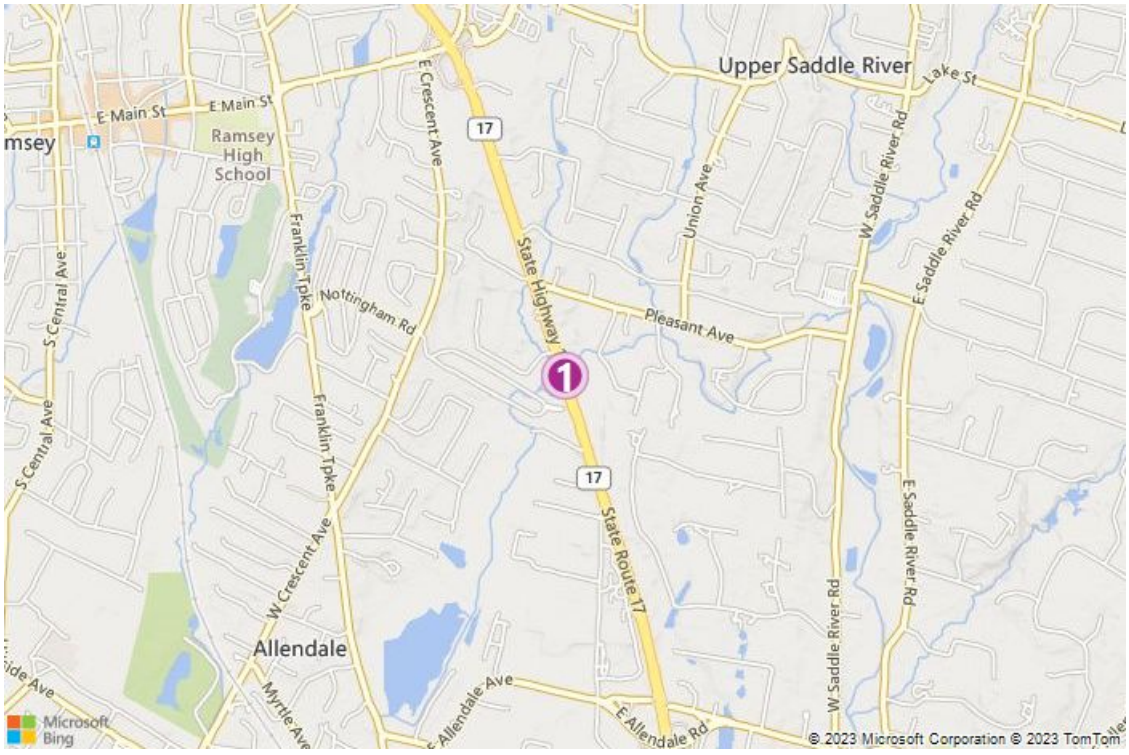
Customer Retention

ALPR PLATE READER RESULT

P ate #	[redacted]	Agency	Bergen County
Date	4/4/2023	T me	4 33 16 PM
Lat/Long	41 04702,-74 11668	Camera	USR-Tra er1-Cam1-ALPR
Nearest	96 State H ghway 17, Upper Sadd e R ver, NJ 07458	Intersect on	State H ghway 17 and Park Way

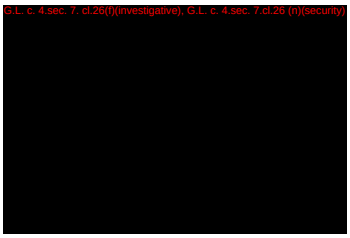


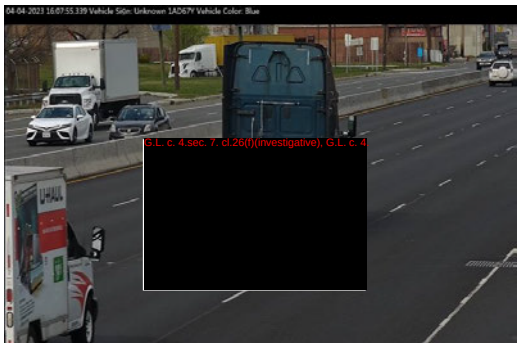


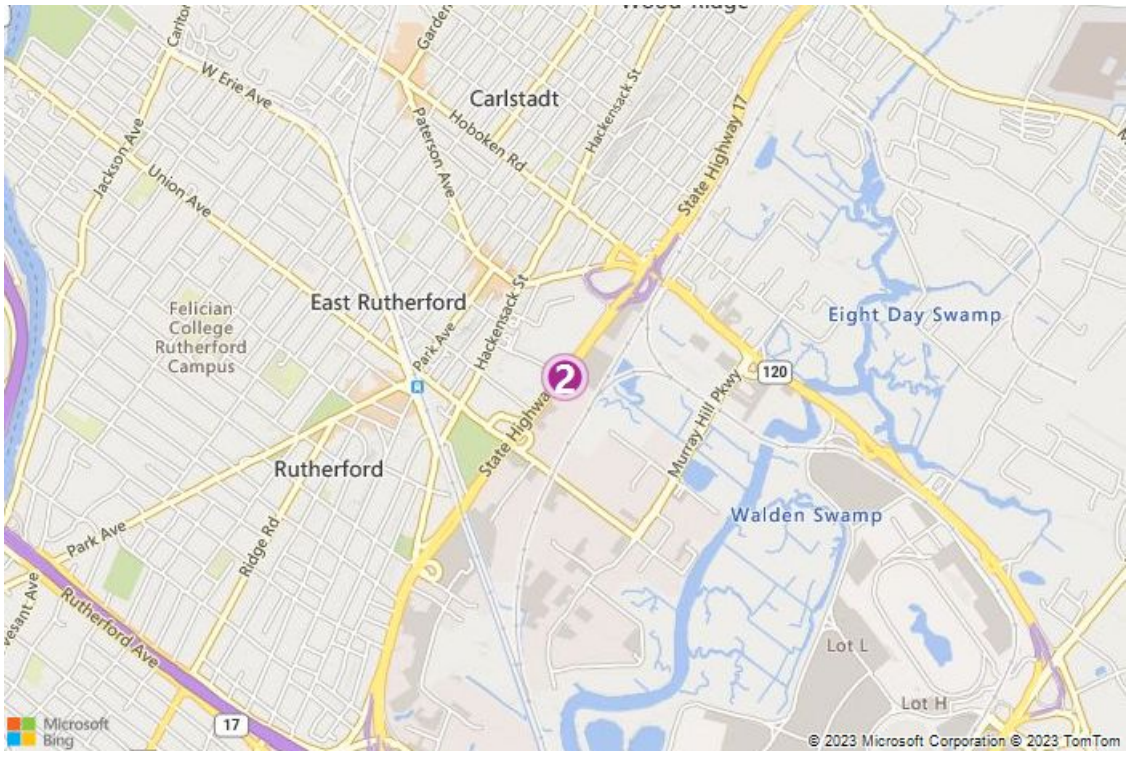


Disclaimer: *The address listed above is only an estimate.*

P ate #	[redacted]	Agency	Bergen County
Date	4/4/2023	T me	4 07 55 PM
Lat/Long	40 8287,-74 09277	Camera	EastRutherford-BCPO-Rt17-N-L1L2
Nearest	150 State H ghway 17, East Rutherford, NJ 07073	Intersect on	State H ghway 17 and Stan ey St







Disclaimer: *The address listed above is only an estimate.*

13.16.02 License Plate Recognition (LPR)

a. Definitions

(1) **LPR:** License Plate Recognition

(2) **LPR System:** Includes a camera and an associated mobile data computer running LPR software, wherein the mobile data computer may exchange data with a central LPR data server.

(3) **OCR:** Optical Character Recognition.

(4) **System Operations Software:** System Operation Software serves as a database, data management tool, inquiry tool, history tracking, and reporting interface for deployed LPR systems.

(5) **Read:** A data file comprised of digital images of license plates and vehicles, and which contains associated data used by the LPR system (e.g., OCR values, date, time, and geographic coordinates associated with the license plate/vehicle image capture).

(6) **Alert:** A visual and/or auditory notice that is triggered when the LPR system receives a "hit" based on an OCR value associated with a license plate.

(7) **Hit:** A read having OCR values corresponding to license plate values that have previously been placed in a hot list.

(8) **Hot list**: License plate values associated with vehicles having law enforcement relevance, for example, stolen cars, vehicles associated with AMBER/SILVER Alerts, as well as vehicles related with criminal activity.

(9) **Mobile LPR system**: LPR systems which include cameras that are affixed, either permanently (hardwired) or temporarily (e.g., magnet-mounted), to a law enforcement vehicle.

(10) **Portable LPR system**: LPR systems which include cameras that can be temporarily deployed in stationary locations which include traffic barrels or speed radar signs.

b. Overview

(1) LPR systems utilize specialized cameras to capture license plate images and use computers to perform OCR on those images such that the OCR values can be compared to a stored list of license plates values. The stored license plate value list is referred to as a hot list. The hot list contains license plate values associated with vehicles having significance to law enforcement, for example, license plates associated with stolen vehicles, vehicles associated with wanted or missing persons, vehicles associated with AMBER/SILVER Alerts, as well as those reasonably believed to be involved with criminal activity. LPR systems include mobile LPR systems, mounted on police vehicles, and portable LPR systems that can be deployed in temporary stationary locations.

(2) The DESPP's LPR system operations software serves as a database, data management tool, inquiry tool, history tracking, and reporting interface for deployed LPR systems. The DESPP's LPR system operations software is installed on a system operations server located at the DESPP Headquarters, and is maintained by DESPP personnel.

(3) The system operations software operates within a secured networked environment that allows license plate read data access to only authorized personnel. The system operations software receives all LPR reads collected by DESPP mobile and portable LPR systems, and organizes the data into a central database. This central database supports a reporting and query function in which authorized DESPP personnel have the ability to:

(a) Search for LPR reads that may match a license plate or partial license plate;

(b) Generate maps showing the location of LPR reads and alarms;

(c) Create metrics based reports utilizing LPR reads and alarms; and

(d) Segregate LPR reads and alarms associated within geographic or time based boundaries.

c. <u>Policy</u>

(1) **Use, Installation and Maintenance**

(a) LPR systems facilitate access to such things as stolen vehicles and wanted person files for the purpose of supporting criminal investigations. As such, the operational use of LPR systems is restricted to authorized users for official law enforcement purposes.

(b) Mobile and portable LPR systems may only be used in vehicles or locations approved by the Commissioner or his designee.

(c) Designated DESPP personnel shall be responsible for the installation and maintenance of the LPR system equipment in DESPP vehicles or temporary locations, and shall be specifically responsible for the installation and maintenance of the system operations software on the system operations, mobile data computer, and all computer hardware and software related to the LPR systems.

(d) Designated personnel shall be responsible for maintaining a detailed inventory record of all LPR system equipment in the custody of DESPP.

(e) Designated personnel shall be responsible for conducting an annual physical inventory of all LPR system equipment and reconciling that physical inventory with the detailed inventory record.

(f) LPR equipment shall be cleaned and maintained according to the manufacturer's recommendations.

(g) Any damage to LPR systems shall be reported immediately according to established DESPP policy and procedures related to the loss/damage to DESPP equipment.

d. <u>DESPP LPR Program Administrator</u>

(1) The Commander of the Bureau of Infrastructure, Transportation and Communication shall designate a DESPP LPR Program Administrator who will be responsible for the overall management of LPR data collection, maintenance, searches, and retention related to the DESPP's LPR systems. The DESPP LPR Program Administrator is also responsible for ensuring all hot lists are updated in a timely manner. The LPR Program Administrator will serve as the LPR systems custodian and shall:

(a) Oversee and administer the storage and management of all LPR data;

(b) Ensure all hot lists are updated in the system operations software and are transmitted to the portable and mobile LPR systems as necessary;

(c) Ensure stored data is purged from the LPR system operations software 90 days after it has been initially stored, and ensure that purging operations are immediately suspended upon the LPR data becoming subject to a preservation or other legal retention obligation involving the LPR data.

(d) Designate personnel who will be authorized to access the secure data collected on the systems operations software server and conduct LPR stored data queries;

(e) Ensure appropriate training of all DESPP personnel that utilize DESPP's LPR system operations software prior to those personnel using the system;

(f) Ensure all training is documented; and

(g) Ensure ongoing training of personnel is provided as needed.

e. Hot List Updating and Storage

(1) The DESPP LPR Program Administrator or designee shall be responsible for updating the LPR system hot lists pursuant this policy. Designated personnel shall be contacted immediately if problems are encountered with the updating of any LPR system.

(2) Each hot list shall be retained for a period of time corresponding with the retention of the LPR systems reads that were compared against that hot list.

f. Data Collection, Retention, and Dissemination

(1) Data collected by the DESPP LPR systems will be maintained on the system operations server utilizing the system operations software.

(2) Only trained personnel approved by the LPR Program Administrator may access LPR system data on the system operations server.

(3) LPR data on the system operations server shall be stored for a period not to exceed 90 days from the creation date, unless such data becomes subject to a preservation obligation or other legal obligation requiring retention. All hot lists shall be retained for a period of time coterminous with the retention of the LPR systems reads that were compared against that hot list. In the event that LPR system read data becomes subject to a legal obligation to retain, the associated hot list shall also be preserved.

(4) In those circumstances when a retention obligation arises, purging will be immediately suspended with respect to the data subject to the obligation.

(5) In the event that LPR data is retained as evidence in an investigation, the data shall be subject to the same DESPP logging, handling, and chain of custody requirements as other electronic evidence.

(6) All requests for data stored on the system operations server shall be considered in view of applicable law, statute, regulation, and policy.

(7) Each request for access to data will be recorded on an LPR Program Data Query Log indicating the date received, the name of the DESPP employee processing the request, and the final status of the request.

(8) The authorized personnel conducting the LPR data query must make the LPR Program Data Query Log entry. The LPR Program Data Query Log shall be retained for a minimum of current calendar year plus one year.

(9) Random audits shall be conducted on the use of the LPR data.

g. Mobile and Portable LPR Systems

(1) Mobile LPR systems will be installed in DESPP vehicles and deployed as directed by the Commissioner or designee.

(2) Portable LPR systems include LPR cameras that are transportable and which can be deployed in a variety of venues as needed. For example, portable LPR systems can be used in conjunction with such things as traffic barrels or speed radar signs.

(3) Commanders of personnel who are assigned mobile or portable LPR systems shall:

(a) Select the appropriate personnel to utilize LPR systems;

(b) Ensure the LPR systems are properly deployed and maintained;

(c) Maintain an adequate number of properly trained personnel;

(d) Ensure all personnel assigned, utilizing, or maintaining LPR systems are properly trained prior to accessing the system;

(e) Designate a supervisor as the Troop LPR program supervisor;

(f) Ensure all required LPR program logs and records are properly maintained according to policy;

(g) Ensure all incidents that involve an LPR hit and arrests that are related to LPR usage are properly documented in CAD by utilizing an LPR sub type; and

(h) Be responsible for overseeing the LPR systems assigned to personnel under their command and ensuring compliance with DESPP policy.

(4) A mobile data computer associated with a mobile or portable LPR system will provide access to current LPR reads and will store a most recent version of the hot list. License plates captured and processed by the LPR system will be stored and accessible utilizing the mobile data computer. LPR data is maintained on the mobile data computer for the purpose of querying the hot list and verifying hits before that data is transmitted to the DESPP system operations server running the system operations software. Such transmission to the DESPP system operations server shall take place no later than the end of shift during which the LPR system was utilized. Mobile data computers will maintain no LPR reads unique to those on the system operations server after the completion of the shift during which the LPR system was used.

(5) Hot lists shall be updated as necessary by the DESPP LPR Program Administrator or designee; however, an update shall be made at no greater interval than once daily. The updated hot list will be transmitted to the LPR systems. The mobile data computer associated with the mobile and portable LPR systems will automatically purge all prior hot list data upon completion of the data transfers.

(6) All data scanned by the LPR system is transmitted to the mobile data computer and compared against the hot list. In the event that a possible match is made between the read and the hot list, an alarm is initiated. When an alarm is received alerting personnel of a potentially hit, a read record will be displayed on the mobile data computer screen. Such read record will include a digital image of the captured license plate.

(7) Personnel who receive an alarm of a hit shall compare the digital image of the license plate to the NCIC information to verify the hit. Verified hits shall be accepted by activating an "accept" alarm key displayed on the mobile data computer screen. When an alarm does not result in a verified hit, personnel shall activate the "reject" alarm key.

(8) Personnel shall provide the information by radio to the local barracks, who shall attempt to confirm the hit according to current policy.

(9) When a trooper locates a vehicle related to a hit, the trooper shall verify the license plate information and relay this information to the troop who will confirm the hit according to current DESPP policy.

(10) Personnel assigned mobile or portable LPR systems shall be responsible for the following:

a. Logging onto DESPP's LPR system to activate the system and receive updated "hot lists" at the beginning of each shift.

b. Ensure that personnel who receive a hit on a scanned license plate compare the digital image of the license plate to the NCIC information to verify the hit.

c. Providing information by radio to the Troop desk operations who shall attempt to confirm the hit according to established policy.

d. Confirming a hit according to established policy prior to any enforcement action being taken.

e. Adding specific information after the initial upload of the fixed LPR system only if it becomes necessary, such as in cases where crimes are reported after the LPR has been deployed (e.g. stolen vehicles, AMBER alerts, SILVER alerts, radio item broadcasts, etc.), or when a manual plate check needs to be performed.) Such updates shall be uploaded to the system operations server automatically, and such update will result in the generation of an updated hot list that will be transmitted to each deployed LPR system in use.

f. Ensuring that all custom manual inputs have a specific criminal investigative or patrol purpose.

g. Ensuring that all data from the mobile LPR system is transferred to DESPP's LPR systems operations server.

h. <u>Hit Verification</u>

(1) The LPR system does not interface with real time COLLECT and NCIC data.

(2) It should be recognized that information derived from license plates is compared against information on the hot list which may be up to 24 hours old.

(3) Personnel must verify all hits through COLLECT and NCIC and follow all DESPP policies and procedures.

(4) The LPR system is ONLY to be used as an investigative tool. Confirmation is essential prior to a stop.

16.1.3 Selective Traffic Enforcement

a. Traffic law enforcement will not eliminate all traffic accidents
Sometimes driver behavior, improper highway construction or design and sudden mechanical failures are not possible to prevent through traffic law enforcement efforts.

(1) **Use selective traffic enforcement programs**
Traffic accidents are most effectively reduced by selective traffic enforcement programs performed by motivated, well trained and properly deployed troopers.

(2) **Department programs cannot perform in a vacuum**
Traffic law enforcement can be relatively successful if there is public acceptance, judicial recognition and fairness in the application of traffic enforcement efforts.

(3) **Traffic enforcement programs must be efficient**
Because of the magnitude of traffic problems and limited personnel resources of the department, troopers must be deployed selectively.

CALEA 1.2.7 **b. Traffic enforcement allows considerable trooper discretion**

(1) The uniform application of traffic laws is an important component of a troop or traffic unit selective enforcement program.

(2) Conducting stationary radar activities in the same spot without consideration for the number of accidents at that location will do little to improve accident reduction, but will cause public antagonism toward these efforts.

(3) Enforcement activities should be directed towards the locations and times that violators are determined to be causing the most accidents or the most serious accidents.

CALEA 61.1.1b **c. Implementing a selective traffic enforcement program**

(1) **Determine enforcement needs**
Commanders and supervisors must accurately analyze the accidents within the troop area to determine when and where they occurred during the previous three year period, using I-CAD / I-LEADS data.

CALEA 61.1.1c (2) **Establish high visibility patrols**

CALEA 61.1.6 (a) Maintain high visibility area, line, or directed patrols because motorists automatically evaluate driving behavior whenever a patrol vehicle is in view.

(b) Active patrols encourage motorists to believe that traffic violators will incur enforcement action.

CALEA 61.1.1d (3) **Deploy traffic enforcement personnel**
The Traffic Coordinator shall deploy traffic personnel to best advantage consistent with unit goals and objectives consistent with the department mission statement.

CALEA 61.1.1c (4) **Conduct patrol activities during peak traffic periods**.
Mobile patrols are a greater deterrent because more drivers will observe a trooper on moving patrol.

(a) By patrolling during peak traffic periods, a high deterrent effect can be realized; but

CALEA 61.1.6b (b) During periods of extremely high traffic density, fixed traffic posts at strategic locations may prove effective, whether covert (hidden) or overt (highly visible).

(5) **Troopers should constantly initiate violator contacts**

(a) Troopers must observe speeders and other hazardous violators to initiate enforcement action.

(b) Drivers witnessing such enforcement activity will believe that patrols are both active and effective.

(6) **Employ random patrol patterns**
Random patrolling should normally be used because predictable patrol patterns allow motorists to anticipate troopers at locations at given times and adjust their driving behavior accordingly.

d. **Types of department patrols**
Which patrol to use will depend largely upon the results of analysis of accident patterns in an area.

(1) **Line patrol**
A line patrol covers a highway from one point to another;

(2) **Area patrol**
An area patrol may include several highways on which hazardous violations have been observed;

(3) **Point or stationary patrol**
Point or stationary patrols are of value whenever a great number of vehicles pass a given location on a highway; and

CALEA 61.1.6c (4) **Unmarked vehicle patrol**
Unmarked vehicles discover hazardous moving violations, which normally would not occur in the presence of a marked vehicle.

CALEA 61.1.1e **e.** **Evaluating selective enforcement efforts**

(1) Any motorist who observes a trooper will usually show improvement in driving behavior because of a perceived risk of penalty for unsafe or unlawful driving maneuvers.

(2) If a trooper observes a violator and takes action, the deterrent effect on drivers who witness the traffic stop is great and long lasting, but if violators are seldom stopped, there will be little or no deterrent effect.

(3) Consistent motor vehicle law enforcement activities by troopers foster the belief among drivers that there is a real possibility of being stopped for a traffic violation.

(4) Compliance with traffic laws can be achieved by earning a reputation for effective traffic enforcement programs and activities.

(5) The degree and quality of enforcement activities will determine the immediate and long term effect of department enforcement programs.

(a) The number of troopers on patrol and the number of arrests and warnings issued are simply measures of enforcement activity.

(b) How enforcement effort is applied will determine the results.

(6) Enforcement efforts which concentrate on violations causing accidents at locations and times when and where accidents are known to occur should reduce the rate and severity of traffic accidents.

(7) Periodic evaluation of enforcement efforts should be conducted at least annually, including tabulation of enforcement action and correlation of enforcements to the number and severity of accidents occurring before and during the program.

f. **Improper motives are counter-productive**

Enforcement programs based upon raising funds or issuing a large number of summonses will antagonize the public, cast doubt upon department credibility and engender disrespect from troopers and citizens.

(1) Efforts must be directed primarily toward selective enforcement of violations which cause accidents.

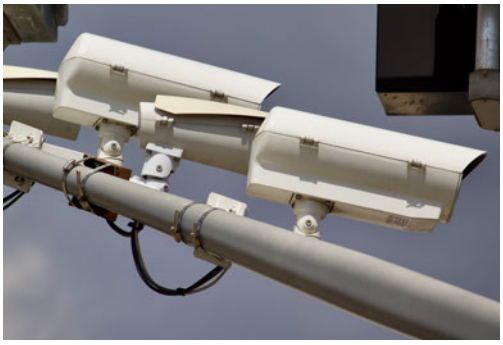
(2) Qualitative and quantitative measurement of activities can be used to measure program effectiveness.

1473

AAMVA

American Association of
Motor Vehicle Administrators

technology
POLICY security
Safety training
REVENUE Data
ACCURACY



License Plate Reader Program
Best Practices Guide





October 2021

LAW ENFORCEMENT STANDING COMMITTEE
VEHICLE STANDING COMMITTEE

2021 © Copyright All Rights Reserved
American Association of Motor Vehicle Administrators

Cover photo credits: © iStockphoto.com

Contents

Executive Summary 2

Chapter 1 Introduction 3

Chapter 2 License Plate History 5

Chapter 3 License Plate Reader Fundamentals 9

Chapter 4 License Plate Reader Benefits 17

Chapter 5 License Plate Readers as a Tool to Improve Toll, Commercial Motor Vehicle, and Border Operations 20

Chapter 6 License Plate Reader Program Best Practices for Law Enforcement 24

Chapter 7 License Plate Reader Success Stories 28

Appendix A Significant License Plate Reader Court Cases and Applicable Federal Statutes 30

Appendix B Additional License Plate Reader Resources 34

Appendix C Sample License Plate Reader Policies 35

Appendix D AAMVA License Plate Reader Working Group Roster 49

Executive Summary

Since their inception more than a century ago, license plates have primarily been used to display information for fast and accurate identification of motor vehicles and to demonstrate compliance with motor vehicle registration laws.

In support of their highway and public safety missions, License Plate Readers (LPRs) provide law enforcement with the ability to check license plates against various databases. Tolling and parking enforcement authorities also rely on LPR technology for the collection of tolls and enforcing parking regulations.

Law enforcement agencies can build meaningful LPR system policies that respect individuals' privacy rights while providing authorized users with the information necessary to ensure the public's safety.

More than a decade ago, it was recognized that inconsistent business rules used by license plate issuing authorities were resulting in alarmingly high "misreads," diminishing law enforcement's ability to identify and apprehend suspected criminals and terrorists, recover stolen vehicles, and assist people in need of assistance. Similarly, tolling and parking authorities are hampered in their revenue collection mandates that are critical to maintaining infrastructure and ensuring parking regulations are not flouted. In addition, license plate misreads hamper Customs and Border Protection's ability to correctly identify vehicles crossing international borders.

In response to this issue, in 2012, AAMVA published a *Best Practices Guide for Improving Automated License Plate Reader Effectiveness Through Uniform License Plate Design & Manufacture*. At the time, AAMVA did not have a License Plate Standard. Since that time, AAMVA has published a License Plate Standard (2016) and a License Plate Standard, Edition 2 (2020).

In 2020, the AAMVA Law Enforcement and Vehicle Standing Committees determined the 2012 LPR document should be retained but with content now covered in the License Plate Standard removed and the remaining material updated and added to as appropriate. This guide has been renamed *License Plate Reader Program Best Practices Guide* and has been refocused on best practices in the administration of LPR Programs for state and provincial law enforcement, although much of the content is applicable to tolling and parking enforcement authorities alike.

Chapter 1 Introduction

License Plate Readers (LPRs) are an effective law enforcement and traffic safety tool and are critical to government entities—such as tolling and parking enforcement authorities—who use the technology to enforce the law and collect revenue. LPRs enhance public safety and security by providing law enforcement the ability to check license plates against databases such as the National Crime Information Center. The databases searched are at the discretion of each law enforcement agency using LPR technology.

Federal, state, local, and tribal public safety agencies rely on accurate and timely license plate information to effectively and efficiently perform the multiple tasks required in the performance of their duties. Information is available in multiple formats, including hot lists (e.g., stolen vehicle), Be On the Look Out (BOLO), Attempt to Locate (ATL), officer safety information, AMBER Alerts for at-risk children, SILVER Alerts for at-risk adults, and more. Much of this information can be, and often is, associated with a vehicle's license plate. The ability of LPRs to quickly and accurately scan thousands of license plates is critical to the men and women of law enforcement who contact hundreds of thousands of people throughout the U.S. and Canada every day, as well as to Customs and Border Protection officers and agents monitoring international ports of entry. When LPRs misread license plates, law enforcement is hampered in its mission to protect and to serve, and government entities lose revenue from uncollected tolls.

The International Association of Chiefs of Police conducted a 2021 survey of police agencies across the U.S. about their use of LPR systems. More than 1,200 agencies responded to the survey measuring LPR use, policy considerations, data retention and management, and more.[1]

Among all respondents:

- **40%** reported currently using LPR systems in their departments.
- Cost was the biggest barrier to LPR use.
- Larger agencies were more likely to use LPR systems than smaller agencies were.
- Mobile units were the most common form of LPR system used.

Among agencies using LPR:

- **75%** owned their own LPR system. Others contracted use of their LPR system or leveraged another agency's LPR system.
- **63%** shared their system with another agency, and **84%** shared their LPR data with other agencies.
- **64%** reported full control of the data in their LPR system.
- **44%** of the agencies using LPR stored their data on the cloud, and **43%** stored their data on agency servers or other government resources.

A study conducted by the Police Executive Research Forum[2] concluded that LPRs increased license plate reads by a factor of more than eight. What the study did not, and could not reveal, is the number of hits "missed" because of license plate misreads. Regardless of the misread rate in a particular jurisdiction, there

1 As of this printing, these represent preliminary estimates only.

2 Combating Auto Theft in Arizona: A Randomized Experiment with License Plate Recognition Technology: Police Executive Research Forum, December 2011.

is no refuting that misreads occur. And when they do, the potential exists to miss opportunities to arrest a suspected criminal or terrorist, to recover a stolen vehicle, or to collect toll revenue.

A completely effective "ecosystem" is needed to ensure as close to 100% as possible accurate license plate read rate is achieved by LPRs. Multiple stakeholders share the responsibility for maintenance of the ecosystem. Motor vehicle agencies having license plate design and manufacture administration oversight responsibility should ensure their issued license plates align with the AAMVA License Plate Standard (see Appendix B). LPR manufacturers have a responsibility to develop and implement state of the art technology to accurately read the multi-variant license plates that exist. Law enforcement and other government entities using LPR are responsible for ensuring they have policies and training that align with the most current best practices available.

AAMVA published a *Best Practices Guide for Improving Automated License Plate Reader Effectiveness Through Uniform License Plate Design & Manufacture*. At the time, AAMVA did not have a License Plate Standard. Since that time, AAMVA has published a License Plate Standard (2016) and a License Plate Standard, Edition 2 (2020) (see Appendix B).

In 2020, the AAMVA Law Enforcement and Vehicle Standing Committees determined the 2012 document should be retained but with content now covered in the License Plate Standard removed and the remaining material updated and added to as appropriate. This guide has been renamed *License Plate Reader Program Best Practices Guide* and has been refocused on best practices in the administration of LPR Programs for state and provincial law enforcement, although much of the content is applicable to tolling parking enforcement authorities alike.

AAMVA also has four policy statements addressing license plates (see Appendix B).

In 2020, AAMVA launched the License Plate Verification Program (LPVP). The LPVP allows jurisdictions to submit up to four license plates per fiscal year for examination and comparison with the AAMVA License Plate Standard, at no cost to the jurisdiction. The examination is conducted by an independent third-party laboratory under contract with AAMVA. A written report is provided to the submitting jurisdiction outlining areas where their license plate(s) do, and do not, align with the License Plate Standard. The report identifies for jurisdictions areas for potential improvement in the readability of their license plates.

This LPR Program Best Practices document, combined with the AAMVA License Plate Standard, Edition 2; License Plate Policy Statements; and License Plate Verification Program all serve to assist jurisdictions in shaping of jurisdiction laws and regulations and operational policies ensuring license plate readability and integrity.

Chapter 2 License Plate History

Introduction

Since their inception more than a century ago, license plates have primarily been used to display information for fast and accurate identification of motor vehicles and to demonstrate compliance with motor vehicle registration laws. The advancement of manufacturing technology has resulted in more colorful and detailed graphics on plates, which can be used to promote a jurisdiction or organization but at times have created an identification challenge for law enforcement and a readability challenge for camera technology. Most jurisdictions now have numerous plate types and designs available to the public.

Hand-Made, Horse-Drawn

The first record of a registration plate in the U.S. was in Philadelphia, Pennsylvania, in the 1850s. Even then, legibility of plates was a concern, and horse-drawn vehicles required registration to be identified with numbers "not less than four inches high." Among other things, these numbers provided a means of identification when reporting an incident involving inappropriate or reckless driving. Today, only the state of Indiana still requires a license plate on a horse-drawn carriage.

The construction of these early registration plates was left to the innovation of the vehicle owner; wood, brass, or other metals affixed to leather backings were common materials used. During the next 50 years, many cities required registration, and they frequently required payment of a modest registration fee.

Plate Production and Issuance

In the early 1900s with the advent of motorized vehicles, jurisdictions took responsibility for registration and standardization of plate issuance.

In 1901, New York became the first state to require license numbers on motor vehicles. In 1903, Massachusetts was the first state to issue a standard statewide plate. Others soon followed, but issuance of plates remained inconsistent.

California also began requiring plates in 1903 but did not produce them; the Automobile Club of Southern California (an early AAA organization) issued license plates—called mouse ears—to members for $1.00. The state assumed this responsibility in 1910.

On March 22, 1905, the Maine senate debated House Document 552, which required automobiles to be registered and plates to be issued. A senator argued in favor of the plate by stating: "The point upon this bill comes is upon the matter of registration. What does it mean? The matter of registration does not prevent the violation of the law, but the matter of registration, and the law compelling the carrying in a conspicuous position, of a certain number, which leads to the registration and which may lead to the detection or recognition of a violation of the law, is all that registration can amount to as to guarding the safety of the public against accidents from automobiles."

As the debate continued, another senator voiced his support for the display of a number on automobiles so that the operator could be identified when it frightened a horse. In part he stated, "I do not own

an automobile, and do not ever expect to. I do own a cheap horse and have a wife and three girls that drive it. What is the result now? They do not dare to go out. I have a safe horse, but when one of those reckless fellows comes along (*in an automobile*), they are likely to get tipped out, as many have in the State of Maine."

The debate continued, the bill passed and became public law Chapter 147. It required the Secretary of State to license operators, to register automobiles and motorcycles, and to issue plates. The law also required the Secretary of State to "furnish the applicant two enameled iron plates containing the word 'Maine' and the number of the registration in Arabic numerals not less than four inches in height. The number plates must be attached to the front and back of the automobile and one number plate must be attached to the back of motorcycles."



Maine plate, 1905 to 1911. The width changed based on the number of characters on the plate.



Starting in 1903, "mouse ear" plates were sold for $1 by the Automobile Club of Southern California.

By 1915, nearly all jurisdictions issued license plates on an annual basis and charged a registration fee that allowed a vehicle to be driven on public roads. Government officials recognized early on that a registration system provided for vehicle identification and a source of transportation revenue. However, license plate design continued down an inconsistent path. It wasn't until 1956 that a standard plate size (12" x 6") was introduced at the request of automobile manufacturers to make it easier to incorporate license plates.

Integrating Safety Concepts

With the rapid increase in the motor vehicle population in the 1920s and 1930s, traffic crashes increased dramatically, leading to the need to improve not only vehicle identification but also vehicle safety. License plates became one means to improve safety by providing a device that improved the night visibility of motor vehicles. The first retro-reflective license plates in the U.S. were issued by New Mexico in 1936.

As retro-reflective technology advanced, fully retro-reflective plates became possible and the first was issued by Connecticut in 1947 followed by Maine in 1949. Delaware followed suit in 1950 followed by Rhode Island and Oregon in 1951.

During the 1950s, relatively new sheeting gave retro-reflective plates their biggest boost. Minnesota had the distinction of being the first state to use the sheeting on automobile license plates.

The effect that retro-reflective plates had on nighttime motor vehicle crashes was dramatic, and it did not go unnoticed. In 1956, the first year of use in Minnesota, deaths caused by automobile crashes in rural areas dropped from 24% to 9%. Urban area fatalities involving parked vehicles decreased from 28% to 7%.

Standards Materialize

Tiny San Marino—the smallest republic in Europe, with an area of only 24 square miles—had the distinction of being the first country on that continent to make reflective license plates mandatory on all 2,500 of its automobiles. In the other hemisphere, the South and Central American countries of Peru and Costa Rica also became pioneers in retro-reflective license plates. In Canada, the provinces of Newfoundland and Alberta led the way. Today, all 50 U.S. states and most other countries in the world use retro-reflective plates.

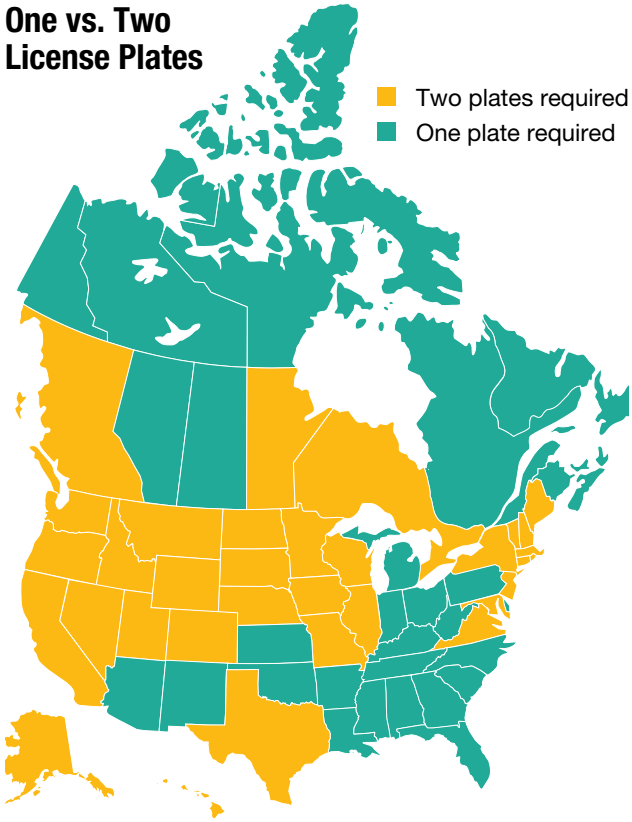
With the advent of retro-reflective license plates, law enforcement realized a benefit in improved legibility.

Although one of the original intents of a vehicle registration number was to aid law enforcement, the reality was that non-reflective plates could only be easily read during daylight hours. Retro-reflection provided greatly improved legibility at night, and even today fully retro-reflective plates continue to have strong endorsement from U.S. law enforcement officials, who advocate fully retro-reflective plates on both the front and rear of vehicles for improved safety and law enforcement efficiency.

Although early license plates were often homemade or devised of porcelain, steel became the predominant base material for plates during the first half of the 20th century. Today, aluminum dominates as the material used in license plate manufacture.

After 1945, most states returned to the pre-war practice of requiring two plates per vehicle. Since then some states have moved from two plates to one or vice versa. States typically move to one plate with the intent to save on the cost of the second plate. During the late 1980s, Connecticut was the last state to move from one plate to two plates. Law enforcement effectiveness was cited as the primary reason for the change. The U.S. and Canada are two of a small number of countries that allow one plate. The following chart identifies the North American jurisdictions that require either one or two license plates.

Within the U.S. and Canada, each jurisdiction is responsible for issuing license plates for vehicles registered in their jurisdiction. To create a plate unique and easily recognizable to that jurisdiction, combinations of colors were originally used. Plate background color and colors of the alphanumeric were varied, along with the characters, to create the necessary combinations needed for vehicle classifications and to differentiate plates among the jurisdictions. With increases in vehicle populations and registration classifications, color alone was not enough. Graphic technology became available in the early 1970s that allowed another level of differentiation of license plates. In 1973, Illinois was the first state to use graphics preprinted on the reflective sheeting, for a special plate for disabled veterans. South Dakota quickly followed with the first general issue graphic of Mount Rushmore National Monument. Today all jurisdictions use graphic plate design. When first introduced, graphic design plates were viewed as attractive and as a mechanism to enhance the image of the jurisdiction.



Three Canadian jurisdictions require two plates and 10 require one plate. Thirty U.S. States and the District of Columbia require two plates and 20 states require one plate. NOTE: The five U.S. Territories are not included.

However, since the proliferation of graphic plate designs, law enforcement is no longer able to easily recognize the issuing jurisdiction. The widespread use of graphics and colors frequently makes legibility of the plate characters a challenge for law enforcement.

Modern Features, Security, and Function

Until the 1990s, all the U.S. and Canada and most of the rest of the world produced license plates with raised (embossed) alphanumeric characters. In the late

1990s, digital printing technology was introduced, resulting in flat, digitally printed license plates. Today, many states are issuing flat plates. Some jurisdictions issue a combination of embossed and flat plates.

As a result of increasing concern with the use of counterfeit license plates used to perpetrate crimes, security features were added to license plate. These security features allow for easy recognition of fraudulent plates and provides one more obstacle for criminals to overcome.

The following functions of a license plate have been, and continue to be, the most important over the past century:

- Display of information necessary for fast and accurate identification of a motor vehicle and compliance with motor vehicle registration laws
- A validation sticker is issued in most jurisdictions, often rotating the color, to indicate a current and valid registration
- Provide an added margin of visibility and safety by making vehicles more visible

More recently, additional functions of license plates have emerged to

- Provide revenue for highway funds and sponsoring organizations (specialty and vanity plates)
- Use images of plates to improve and increase toll collection, parking fees, and fines
- Provide a way for individuals to express their pride or to promote various causes
- Provide access control to parking, facilities, and gated communities.

Alternative Vehicle License Plates

Two nontraditional license plate technologies have recently emerged: digital license plates and front license plate wraps. These alternative vehicle license plates are intended to replace traditional aluminum or metal license plates.

Digital license plates are reflective but not retro-reflective, creating challenges for law enforcement, tolling authorities, and others that read license plates in all light conditions and rely on License Plate Reader (LPR) technology, which is currently programmed to read retro-reflective license plates.

A license plate wrap is an adhesive license plate applied to a vehicle's bumper. Wraps, where currently authorized for purchase, are only allowed to be applied to the front of a vehicle.

A curved, indented, or otherwise non-flat surface could render the wrap unreadable to LPRs or the human eye.

For a fuller explanation of both the benefits and challenges associated with nontraditional license plates, see the AAMVA License Plate Standard, Edition Two, Chapter 5 – Alternative Vehicle License Plate Displays.

Chapter 3 License Plate Reader Fundamentals

Introduction

This section provides an overview of License Plate Readers (LPRs), the license plate reading process, and key challenges faced by LPR systems.

Typical applications for LPR technology by law enforcement, motor vehicle administrations, and other entities include but are not limited to:

- Law enforcement stolen vehicle and other "hot list" files
- AMBER, BLUE (violent criminal who has killed or injured a law enforcement officer), and SILVER Alerts
- Open road tolling (pay by plate)
- Congestion pricing
- Parking enforcement
- Access control
- Traffic studies
- Automated speed enforcement
- On-street parking enforcement
- Travel or journey time calculations

As the demand for LPR systems expands in both law enforcement and commercial applications, LPR technology continues to evolve. LPR provides cost-efficient approaches in varied environments that include both environmental challenges (e.g., mobile-based platforms, high-speed traffic) and license plate challenges (e.g., introduction of new designs, fonts, and so on across multiple jurisdictions).

The reads from LPR systems, namely the license plate number and in some applications the license plate jurisdiction, are primarily used as input into downstream systems to support the intended application. For example, whereas in open road tolling systems, the license plate number and jurisdiction are used to support the collection of toll revenues, in federal and state law enforcement systems, the license plate number and jurisdiction are used to support law enforcement queries against both large-scale (e.g., National Crime Information Center) and local data sources.

In some applications, manual verification or certification of LPR results is required at some point in the process. To the extent LPR systems can improve and retain a high degree of accuracy, operational costs can be reduced. In some applications, LPR system service-level objectives call for a 95% accuracy rate in correctly identifying both the license plate number and jurisdiction when the license plate is completely visible in the license plate image. The most significant challenge to maximizing license plate read rate accuracy is the ability of LPR system vendors to quickly adapt to the introduction of jurisdictional license plate designs with varying fonts, graphical designs, stacked letters, and so on.

License Plate Reader Systems

LPR systems include deployment of fixed, portable, mobile, and mobile application platforms.

Fixed Platforms

Fixed LPR platforms are permanently mounted on fixed infrastructure such as overhead gantries or roadside bollards. LPR fixed platforms are commonly used in open road tolling, commercial vehicle weigh station operations, and some federal and local law enforcement applications.



Fixed LPR in weigh station operations.



Fixed LPR in Customs and Border Protection inbound.

Portable Platforms

Portable LPR systems can be transported between locations, assembled, operated, and then disassembled. Once deployed, they operate as a fixed platform. Examples include portable trailers, traffic barrels, and other platforms configured with or containing LPR equipment.



Portable department of transportation trailer with LPR.



Speed trailer with LPR.

Mobile Platforms

Mobile LPR systems are defined as any LPR system that is mounted on a vehicle, whether a police car, tow truck, street sweeper, parking enforcement vehicle, and so on. These systems can include one to four camera configurations and are typically mounted on the roof or trunk, or they are custom manufactured.

Typical components of mobile systems include cameras that obtain images of the plate and vehicle, which in turn are passed to a processor mounted in the trunk. The processor locates the license plate in the image and extracts the license plate number. It then compares the textual license plate read against selected data sources and sends the output in the form of an alert to a mobile data terminal (screen) and an operator in the cab. The alert typically contains the name of the data source to which the image was compared such as an expired license or registration system, an infrared (IR) image of the license plate, and a color overview image of the vehicle in question. Data generated from mobile LPR systems can also be stored or transmitted via a back-office software application.



Patrol vehicle roof-mounted LPR.



Parking enforcement roof-mounted LPR.

Mobile LPR Applications (Apps)

Mobile LPR applications are defined as LPR systems that are held and operated by individuals using devices such as barcode readers, ruggedized PDAs, and smart phones that provide other capabilities (e.g., communications, internet access). These technologies provide mobile LPR capabilities and rely on the user to point the imager toward the location of the license plate.



LPR application on a mobile device.

Use of these devices is limited to speed applications typically less than 45 mph and are subject to unique challenges such as shadows, low ambient light, distance or angle to the license plate surface, and non-reflective surfaces. These limits can be overcome using techniques to light or IR illuminators resident in the device. Because IR imagers are not typically available on commercial general-purpose handheld devices, overcoming readability of non-reflective surfaces using a color imager generally requires special Optical Character Recognition (OCR) techniques. The accuracy of these OCR devices is dependent on the specific device and environment in which it is being used.

Handheld platforms are useful because they are easily deployed and can be used in parking enforcement, covert applications, portable checkpoints, and more. Benefits include portability, relatively low cost, and tactical use. The biggest drawback is that when the LPR application is used, it drains the device battery much faster than normal usage.

LPR Camera Technology

Two primary approaches are used to capture images from which the license plate information can be extracted. One approach is to capture a single still image of the license plate at an "optimal" distance from the camera, where the illumination, lens settings, and field of view can all be controlled to yield the best possible images under any ambient lighting and weather conditions. Another approach is to capture multiple images as the vehicle travels through the field of view of the camera. In this approach, near-instantaneous adjustments to the flash, shutter, and gain settings are performed to optimize the license plate image for different environmental conditions.

Monochrome (black and white), color, and IR cameras are used in various solutions. Monochrome cameras tend to yield the best resolution, can work with most types of visible light illumination, and are generally less costly. Color cameras are useful when the color information can be used to improve

the separation between characters and background and for identification of the jurisdiction. Color cameras require white light to produce accurate color information and are of very limited value at night without the use of additional illumination.

IR cameras are tuned to respond to IR illumination. IR cameras tend to be most sensitive at night and tend to be fitted with a band-pass filter designed to block visible light (to limit the effect of headlights and sunlight). This tuned IR illumination is effective at reflecting off the reflective background finish of the plate and not reflecting off the non-reflective characters (or vice versa).

Additional cameras are often used as part of the solution so that both a plate image and a vehicle image can be simultaneously captured to provide context and for investigative purposes. Multiple cameras are also useful when multiple bandwidths of light are used. For example, the fusing of white light and NIR (near-IR) light imagery adds significant information during the OCR and jurisdiction determination.

License Plate Recognition Process

The license plate recognition process begins when a vehicle is detected by an LPR system and ends when an LPR system information has been collected, analyzed, and handed off to backend systems for further processing.

The key steps of the LPR process are to

- Detect the vehicle and/or license plate.
- Locate the license plate in the image(s).
- Extract license plate characters from the background.
- Identify the license plate number.
- Determine the license plate jurisdiction *(optional).*
- Hand off LPR results to backend systems.

The following paragraphs describe each of the LPR steps in detail.

Detecting the Vehicle and/or License Plate

External triggers such as through-beam IR sensors, retro-reflective license plate sensors, ground-based induction loops, laser range sensors, and so on can be used to detect the presence of a vehicle in the field of view of the ALPR system. These types of triggers are primarily used in fixed-platform ALPR systems. Alternatively, the ALPR system detects the presence of a license plate by analyzing the camera's video signal (which may capture up to 60 images per second) and looking for potential license plate candidates. This type of detection is primarily used in mobile platform ALPR systems and can support vehicle speeds up to 140 mph. When the vehicle is detected, the ALPR captures one or more images containing the license plate that will be used to support the subsequent license plate number and jurisdiction determination.

Locating the License Plate in the Image

After one or more images containing a license plate are captured, a "license plate finder" algorithm is used to determine the exact location of the license plate in the image. This may be accomplished by searching for license plate characteristics (e.g., high-contrast objects) or character strings in the image that indicate the presence of a license plate. This process is one of the most difficult steps of the LPR process because the license plate must be located in potentially conflicting images that contain other information that may appear as license plates (e.g., bumper stickers, other writing, contrasting graphic designs). In addition, the type and condition of the license plate (e.g., retro-reflective, non-reflective, license plate frames and covers, license plate orientation) may require the use of special lighting and camera technologies to both locate and present the optimal license plate image to the character recognition algorithms.

As shown in the picture below, LPR cameras can vary flash, shutter, and gain settings to capture multiple images per vehicle over a wide range of ambient and environmental conditions.

Camera Arrangement	Resulting Image with Unchanged Ambient Conditions
Flash Duration = 130 µs Shutter Duration: = 200 µs Gain = 2	
Flash Duration = 390 µs Shutter Duration: = 500 µs Gain = 2	
Flash Duration = 780 µs Shutter Duration: = 1000 µs Gain = 2	

By varying camera settings and controlling illumination, the ability to locate a license plate within an image can be greatly improved. In addition, the 'best' image can also be used to improve the accuracy of the subsequent character extraction and license plate number determination.



License plate that has been located in the larger vehicle image captured by an LPR camera.

Extracting the Characters from the Background (Segmentation)

After the license plate is identified in the images(s), the region around the license plate may be further analyzed to extract the characters from the background. In the following example, pixels making up the candidate region are separated into foreground and background pixels to provide a more suitable candidate image used by the OCR algorithms to translate a character string image into an alphanumeric value that constitutes the license plate number. This is made more difficult when there is little contrast between the license plate number and the plate background.



The segmented or pre-processed license plate image is then passed off to OCR software, where the images are converted to individual alphanumeric characters.

Determining the License Plate Number

Challenge: Poorly designed fonts and variations in fonts themselves, additional symbols, half-height characters, location of registration stickers, license plate frames and covers, and holograms on characters all increase the complexity of OCR algorithms used to determine the alphanumeric characters of a license plate.



In the following example, you can see the software cannot discern whether the first character is a "B" or and "8" and whether the third character is a "6" or a "G."

In the following license plate examples, the ascender and descender of the letter 'Q' takes on different characteristics that may require specifically tuned or trained OCR engines depending on the region or jurisdiction in which the LPR system is deployed. The number '4' in the first license plate compared with the '4' in the second photo below provides another example of inconsistent fonts used between jurisdictions, making the same number look different. Note that the image processing and segmentation steps described must discern the actual license plate number from other alphanumeric information such as vehicle registration tabs and jurisdiction names and logos.





Determining the License Plate Types and Jurisdiction

Some LPR systems can identify the license plate type and the jurisdiction of origin by recognizing key features on the plate such as the jurisdiction logo, background graphics, special symbols, unique character font features, and so on. Other techniques include applying syntax rules and other regionalization rules to provide additional clues to determine the license plate jurisdiction. Use of white light for this process significantly improves the accuracy of jurisdiction identification. Many of the jurisdiction specific features are lost when imaging the license plate in the NIR light spectrum.



Handing Off LPR Results to Backend System

After the license plate number and, in some cases, the jurisdiction, are determined, the information is handed off to backend systems in support of the intended LPR system application. These systems may compare the license plates with watch lists or other law enforcement systems to allow interdiction or other actions to occur in near real time. Sometimes these actions are not for interdiction purposes but merely to allow vehicles to gain access to secure locations, parking garages, and so on.

In some cases, the LPR data—along with supplemental data such as scene and driver images, vehicle location, and date and time stamps—are stored in highly scalable and searchable data sources to support intelligence analysis, bill generation, or other processes that may occur at a later date.

LPR systems are often configured to automatically communicate or transmit all the collected data to a backend data archive or server. Communication methods can include any conventional networking protocols, including cellular, Wi-Fi, hardwire, and thumb drives, all with a variety of security protocols. In many cases, this communication process occurs in the background without any effort from the system user.

After the data have been inserted into the backend data management software, they are immediately available for review and search. These systems are generally web based and can support numerous workstations simultaneously. Often the software solutions used to manage data sources allows information to be queried in a multitude of ways, by location, time, plate number, and so on.

In addition, the image captured and the results generated by the ALPR system can be digitally signed and encrypted to enable a third party to verify that the data was collected at a specific time and location and that no one has tampered with it. This approach also provides for a chain of custody for legal evidence purposes.

Challenges Associated with License Plate Reading

Certain steps of the LPR process present unique challenges that require continuous innovations in hardware and software technologies. A key challenge is the constant introduction of new and varied license plate designs that greatly expands the types of license plates

that LPR systems are required to process. Some of those challenges and the current techniques being applied to address these challenges include the following.

Detecting the Vehicle and/or License Plate

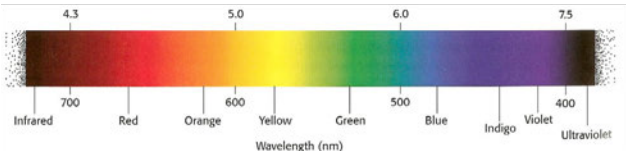
Challenge: LPR systems operate in outdoor environments subject to constantly changing conditions, including lighting, weather, varying vehicle speed and acquisition angles, and varying distances from cameras.

Techniques: LPR camera locations, focal points, illumination controls, and vehicle detection sensors are carefully controlled to help ensure the capture of optimal images used for subsequent license plate location and OCR. Often ALPR cameras are sequencing illumination levels or acquisition parameters to counteract the constantly changing conditions in which they are operating.

Locating the License Plate in the Image(s)

Challenge: Low-contrast license plates, license plate frames and covers, and other noise in the image (e.g., bumper stickers) all impact the ability of license plate detection algorithms to locate the license plate in the larger image captured by the LPR system.

Techniques: Commercial LPR systems typically use a narrow band of IR illumination to light the plate for detection purposes in nearly all weather and lighting conditions. This band ranges from 750 nanometers (nm), which has a visible bright red glow, to 810, 850, 940, and 950 nm. A 950-nm IR illumination is completely invisible to the naked eye.



The purposes in using several bands of IR light are to filter out the effects of background graphics and to highlight the alphanumeric characters for OCR software systems. To help overcome graphic-heavy backgrounds, a spectral analysis can be performed automatically on a plate-by-plate basis to determine which IR illumination is best suited for each plate at the time it is read by the LPR. In general, lower IR bands such as 750 nm handle heavier graphics, and higher IR bands of light are more effective with lower density graphic backgrounds.

Extracting License Plate Characters

Challenge: License plates with conflicting backgrounds or graphics that encroach on the character fields present conditions that make it difficult to recognize specific license plate characters.











Technique: To address these challenges, LPR systems can use different illumination techniques to improve the contrast between characters and background. Also, specialized segmentation algorithms are used to segment the characters from the background. Many LPR systems use neural networks that are trained to find characters correctly in cases of low contrast between characters and background.



In this example, the R could be read as an A and the Q as an O.



The first photo shows a plate with three stacked characters (the AAMVA License Plate Standard calls for no more than two characters to be stacked). The second photo shows appropriate half-height stacked characters. In some jurisdictions, the stacked characters are considered part of the plate number, but in other cases, they are not.



When characters are located too close to the plate's edge, license plate frames can easily prevent the plate number from being read by an LPR.

Chapter 4 License Plate Reader Benefits

Introduction

Prior to the introduction of License Plate Reader (LPR) technology, a law enforcement officer could run a minimal number of plates per shift. LPR technology allows an officer to "read" more than eight times the license plates than officers conducting only manual checks. LPR systems may be used in targeted areas such as crime hot spots, assisting law enforcement in obtaining valuable information of vehicles that may be involved in criminal activity. Moreover, by eliminating the manual check process, not only is officer efficiency increased, but it allows officers to focus more on their surroundings, which improves both officer and public safety.

In studies supported by the National Institute of Justice, research was conducted as to the effectiveness of LPR use for law enforcement patrol and investigations. The first study was conducted in a large suburban jurisdiction in designated hot spots for a period of four months. Officers who used LPR were found to be much more likely to recover stolen vehicles than officers who did not use LPR. The second study examined how LPR could be used for investigations and was focused on a large city with nearly 100 LPRs in fixed locations. After two years, researchers noted 4,000 incidents were documented, including auto theft, missing persons, and homicide cases. LPRs were found to provide information that contributed somewhat to resolving roughly one in five incidents.[1]

Misreads of license plates by LPRs or illegible license plates causing no reads by LPRs do occur.

1 Christopher S. Koper and Cynthia Lum, "Effectiveness of License Plate Readers for Patrol and Investigations," Research in Brief, Police Chief 85, no. 9 (2018): 14–15.

Research conducted by one major toll authority from December 2020 indicated that 9% of toll revenue was lost because of unbillable revenue from misread or illegible license plates.



Gantry mounted LPR technology commonly used for automated toll collection.

When they do occur, the potential for arresting the wrong person, missing an opportunity to arrest a suspected criminal or terrorist, recover a stolen vehicle, or miss toll revenue exists. Research conducted by one major toll authority from December 2020 indicated that 9% of toll revenue was lost because of unbillable revenue from misread or illegible license plates.[2]

Challenges to Law Enforcement

In the past, a law enforcement officer could be familiar with all 50 states' license plates. Today with the proliferation of license plate designs, specialty, and vanity plates—in some cases into the hundreds in a single jurisdiction—it is virtually impossible for instant visual recognition for today's police officer. The issue

2 E470 Public Highway Authority Quarterly Dashboard Report December 31, 2020.

is exacerbated by the introduction of additional new license plate designs each year. Moreover, novelty plates that closely resemble official license plates have added to the difficulty law enforcement contends with in determining plate validity.

A sampling of eight states illustrates the significant growth in the number of license plate designs in circulation in the U.S.

This table represents a sample of the growth in license plate designs:

Jurisdiction	2009	2012	2021
Arizona	52	64	75
California	106	117	167
Maryland	800	935	1,365
Missouri	172	200	269
Montana	152	177	350
Pennsylvania	245	310	582
South Carolina	385	417	429
Texas	225	376	499
8 state totals	2,137	2,596	3,736
% Increase from 2009 to 2021			57%

Officer Safety Benefits

Safety is of paramount concern for any law enforcement officer initiating a "routine" traffic stop. Officers in patrol vehicles that are not equipped with LPR technology may not be as informed about the vehicle and its occupants as those who have the technology.

LPR technology provides the ability to check the vehicle plate number automatically and rapidly against selected databases. License plates are often "flagged" when the owner is associated with certain information (e.g., wanted, attempt to locate, be on the lookout for, stolen car). With LPR technology, officers stopping drivers for sometimes minor traffic offenses can be made aware of this type of information, which allows them to use the appropriate officer safety tactics given the information they have instead of unknowingly walking into a dangerous encounter.

Traffic Safety Benefits

One significant example of a traffic safety benefit involves suspended, *revoked, or otherwise ineligible* drivers. *Across North America, at any given time, approximately 7% of all drivers are suspended, and it is estimated as many as 75% of these people continue to drive.*[1] Moreover, 19% of all fatal crashes involve an unlicensed or suspended driver. These drivers pose a significant threat to highway safety. LPR technology has the capability to quickly identify vehicles whose registered owners have suspended or revoked licenses or registrations, making it much faster and easier for law enforcement officers to detect and apprehend suspended drivers.



Benefits to Law Enforcement: Beyond Traffic Safety

LPR's are at the forefront of discussions about the impact of technology on improving traffic and public safety. In the field of auto theft recovery and investigation, the LPR is a force multiplier for officers in the field. The technology enables reading and checking the status of thousands of license plates in a single shift, all while the investigator can watch his or her surroundings for activity, malevolent or benign. The LPR is a tireless partner, constantly on the watch

1 The National Cooperative Highway Research Program, Report 500, Volume 2.

for stolen vehicles and wanted subjects, AMBER Alerts, missing persons, and more. This technology is even more effective when there is a front and rear license plate for the LPR to read.

Many police agencies use LPR-equipped vehicles to collect plate information as they respond to bank robberies and other major crimes to capture plate numbers of vehicles leaving the area as police respond to the scene of the crime. There have been many instances when these reads have led to the identification of suspect vehicles and suspect arrests.

Public Safety Benefit

As mentioned in the previous Benefits subsections, LPR-equipped law enforcement vehicles can scan thousands of plates an hour, thus increasing the chances of finding a particular vehicle quickly, enhancing highway and public safety. One example was provided by the Utah Department of Motor Vehicles Enforcement Division, which prior to installing LPRs on their police vehicles, averaged



One example was provided by the Utah Department of Motor Vehicles Enforcement Division, which prior to installing LPRs on their police vehicles, averaged 400 stolen vehicle recoveries annually. After LPR deployment, they now scan 45,000 plates monthly and are now recovering more than 1,000 stolen vehicles annually. See Chapter 7 – License Plate Reader Success Stories for many more examples.

400 stolen vehicle recoveries annually. After LPR deployment, they now scan 45,000 plates monthly and are now recovering more than 1,000 stolen vehicles annually. See Chapter 7 – License Plate Reader Success Stories for many more examples.

It should be noted that there are circumstances when the lack of a front license plate limits the effectiveness of LPR on front-facing traffic. This is also an issue for school bus drivers who report drivers who fail to stop for the buses while loading or unloading students. These drivers often rely on the presence of a front license plate to be able to report these violations. Some tolling authorities also rely on the front plate for both revenue collection and enforcement.

Homeland Security Enhancements

LPR technology has also become an important national security tool. LPR technology is used to query the license plate numbers of vehicles entering and departing the U.S. to identify potential threats to national security. LPR units are also set up in locations in proximity to critical infrastructure to identify potential threats.

Chapter 5 License Plate Readers as a Tool to Improve Toll, Commercial Motor Vehicle, and Border Operations

Introduction

This chapter discusses how License Plate Reader (LPR) systems benefit public mobility but also have become core to the way many electronic toll systems collect tolls and enforcing payment. LPR has made it possible for the toll industry to move increasingly toward all-electronic cashless toll operations, which are permitting free-flow traffic to pay tolls at highway speeds, improving roadway efficiency, improving the customer experience, and mitigating adverse environmental impacts. Road and bridge toll collection helps provide revenue assurance for highway lane management, maintenance, and improvement.

LPR systems are also effective in commercial vehicle enforcement, which results in efficiencies in safety and traffic flow near weigh station and inspection facilities. These systems help officers identify and focus resources on the vehicles and drivers that are most likely to present safety risks.

LPR systems are also deployed by Customs and Border Protection along the U.S. borders with Canada and Mexico to improve and enhance traveler mobility across these borders.

The introduction of electronic toll collection (ETC) has reduced the dependence on toll collection personnel and manual cash transactions at toll points. Although ETC has improved traffic flow and efficiency, it has also introduced a new challenge—toll evasion and revenue loss.

Mobility and Toll Collection

Collection of user fees on roads, bridges, and tunnels—or tolls—has served as an important means of financing key transportation projects and funding ongoing operations and maintenance for as long as roads have existed. Tolls provide a direct approach to funding highways, bridges, and tunnels without increasing local or state taxes, and they ensure that those who use and benefit the most from these projects pay for them directly.

For toll facilities to be effective, however, tolls must be collected. Historically, toll collection involved staff at a gate or in a toll booth collecting cash directly from motorists and making change at strategic points along the roadway. This process required each vehicle to stop in the tolling zone for a brief period to tender a cash toll payment. When the collection site becomes a choke point – risks of rear impact and chain reaction crashes increase. Toll chokepoints also reduce the efficiency of the corridor where collection takes place. Additionally, when toll collection slows traffic, the reduced efficiency adds emissions into the environment and increases the time required to move people and commercial goods.

Over the past three decades, most toll operators modernized their toll collection systems with technology that allows for prepaid toll accounts using in-vehicle transponders to identify valid toll account holders. The introduction of electronic toll collection (ETC) has reduced the dependence on toll collection personnel and manual cash transactions at toll points. Although ETC has improved traffic flow and efficiency, it has also introduced a new challenge—toll evasion and revenue loss. Toll violators

include motorists who travel through an ETC-only lane without a transponder or unfunded toll account, creating unpaid toll transactions. This not only reduces the funding available for roadway operations and maintenance but also adversely affects fairness to those who pay their tolls, potentially eroding public support for tolling. In an ETC environment, there is a cash payment option for motorists without a transponder and prepaid toll account. LPR technology is used to capture license plate images of vehicles without toll transponders in ETC toll lanes to enforce the toll payment from the registered vehicle owner.

In recent years, toll operators are increasingly adopting all-electronic tolling (AET) operations, in which the cash payment option is eliminated entirely. Cashless AET operations offer the benefit of allowing free-flow tolling, often permitting all vehicles to move through the tolling point at the posted speed limit without stopping or slowing. AET operations are reducing the need to separate cash payment and ETC vehicles and the associated roadside infrastructure required to do so. Instead, AET operations often use overhead gantries with electronic toll equipment (e.g., antennas, transponder readers, and LPR cameras) to process the toll transaction with all vehicles.

This not only reduces the funding available for roadway operations and maintenance but also adversely affects fairness to those who pay their tolls, potentially eroding public support for tolling.

Vehicles with in-vehicle transponders pay their tolls through their toll accounts, just as they do in an ETC environment. Vehicles without toll transponders in an AET environment have their license plate images captured, and toll bills are sent to the registered owners of the vehicles to arrange payment of the toll due. In an AET tolling environment, more transactions are being processed based on LPR technology. For commercial motor vehicles, the Federal Motor Carrier Safety Administration estimates a truck will save approximately $10 per facility each time a truck is able to legally bypass a weight station or inspection facility.

Today as motor vehicle transportation solutions orient their designs toward improved mobility, reduced congestion, and more reliable levels of service, the use of LPR technologies has increased substantially. The conundrum in this development is that as LPR technologies improve, license plates continue to take on increasingly complex designs, making accurate license plate reading problematic.

According to the Federal Highway Administration (FHWA), jurisdictions throughout the U.S. are installing managed lanes (e.g., high occupancy/toll [HOT] lanes) in response to increased congestion. Managed lanes are intended to lessen congestion and provide greater mobility than the adjacent general-purpose lanes of state highways or interstate highways located in urban areas. In some cases, it is also used to enforce High Occupancy Vehicle (HOV) violations automatically, without the need of a law enforcement officer to visually detect violations. LPR also assists transportation officials to understand and influence traffic patterns and set flexible pricing based on traffic levels to reduce congestion, resulting in fewer roadway incidents and increased mobility.

Today as motor vehicle transportation solutions orient their designs toward improved mobility, reduced congestion, and more reliable levels of service, the use of LPR technologies has increased substantially. The conundrum in this development is that as LPR technologies improve, license plates continue to take on increasingly complex designs, making accurate license plate reading problematic.

Another feature of the move to LPR-related open road tolling is the use of enforcement-intended data access for revenue collection that is not law enforcement related. In jurisdictions where overhead tolling is

introduced, the department of motor vehicles should be consulted in the means by which vehicle and vehicle operator data may be obtained.

Revenue Loss

License plate designs, license plate obstruction, and purposeful avoidance to register and title vehicles are the most significant contributors to revenue losses for authorities using LPR systems. License plates that align with the AAMVA License Plate Standard will improve the effectiveness of LPRs and subsequently increase toll collections.

One toll agency with years of experience in operating a cashless AET operation that depends on license plate images to collect tolls from motorists without toll transponders indicates the following experience:

	2017		2018		2019	
Total Image Transactions	**36.930M**		**39.092M**		**41.143M**	
Reject Reason	**Total**	**%**	**Total**	**%**	**Total**	**%**
Unreadable Plate	2.058M	5.6%	2.139M	5.5%	1.901M	4.6%
Temporary Plate	1.063M	2.9%	723K	1.8%	667K	1.6%
No DMV Record	1.116M	3.0%	801K	2.0%	780K	1.9%
Other	784K	2.1%	1.061M	2.7%	978K	2.4%
Unenforceable Totals	**5.021M**	**13.6%**	**4.724M**	**12.1%**	**4.326M**	**10.5%**
Lost Revenue	**$23.1 Million**		**$25.8 Million**		**$25.3 Million**	

Although the unrecoverable revenue is significant, it should also be noted that even through a 12.1% growth in image-based transactions over three years, there was a 13.8% decline in unenforceable images. This is indicative of what the industry has experienced in terms of improvements in hardware, software, and business practices improving overall outcomes. That said, easily identifiable license plates can further mitigate lost revenue in the transportation industry as well as other businesses and enforcement models that use imagery and license plate information as the core of their revenue enforcement efforts.

Lost toll revenues amounted to $23.1 million in 2017, $25.8 million in 2018, and $25.3 million in 2019.

Mobility at U.S. Borders with Canada and Mexico

Currently, Customs and Border Protection (CBP) has three programs that use LPR to expedite entry to the U.S.—NEXUS, Secure Electronic Network for Travelers Rapid Inspection (SENTRI), and Free And Secure Trade (FAST). NEXUS is used at the Canadian border and SENTRI, is used at the Mexican border. FAST is a commercial clearance program for low-risk shipments entering the U.S. from Canada and Mexico. Each of these programs has dedicated lanes, and users are vetted.

All vehicles and persons entering the U.S. are subject to inspection. Every vehicle and every person entering at a land border port must be queried through various law enforcement databases before they can enter the U.S. Although the inspection process encompasses more than just queries, each query takes time to perform, and time is a factor in vehicle wait times. CBP, through the Western Hemisphere Travel Initiative (WHTI), has installed technology at most ports of entry that automates many functions previously done manually. This automation has resulted in reduced vehicle inspection times while maintaining the integrity of the inspection process.

Other LPR Applications That Benefit Mobility

Commercial Vehicle Enforcement

Commercial Vehicle Enforcement entities use LPR. Several specialized companies have emerged that use LPRs to read license plates and compare the plate number to federal safety data sources to ensure trucks are in compliance with federal and state motor carrier safety programs. Some systems also verify various state and federal credentials required to operate in the jurisdiction, check for out-of-service violations, and check for wants or warrants associated with vehicles.
Municipal Parking Enforcement



LPR camera in use at a roadside truck scale.

Municipal Parking Enforcement

On-street parking enforcement efficiencies have been gained by using LPR technology. With these systems, parking scofflaws who fail to pay their parking citations or fines are placed in a data source that is downloaded to an LPR-equipped vehicle. The LPR quickly identifies those who have failed to pay, which allow municipalities to boot vehicles, ensuring parking revenues are recaptured.



Mobile LPR camera mounted on parking enforcement vehicle.

In a 30-day trial conducted during 2020 using one LPR-equipped vehicle, the Long Beach Police Department in southern California identified nearly 300 scofflaws who had five or more unpaid parking citations, capturing nearly $200,000 in unpaid fines. In addition, seven arrests not associated with a parking citation were made.

Chapter 6 License Plate Reader Program Best Practices for Law Enforcement

Introduction

A properly organized and managed license plate reader (LPR) program can greatly enhance the effectiveness of patrol operations and criminal investigations. The best LPR programs are built on a foundation of good policy and training.

The measurement of success for an LPR program is subjective. Recovering stolen vehicles; arresting subjects with active warrants; and recovering AMBER, SILVER, and BLUE Alert subjects are some measures of success. However, in an era of transparency and civilian oversight, a true measure of success should include an agency's ability to collect, store, and delete millions of LPR reads in an efficient and secure manner. It should also be noted that LPR systems are only as good as the data they rely on. Ensuring that the hot lists they access are kept current is critical to limiting the possibility that users will act on erroneous information.

Policy

Law enforcement agencies can build meaningful LPR system policies that respect individuals' privacy rights while providing authorized users with the information necessary to ensure the public's safety. Policies should include LPR program goals and objectives and should not be too restrictive as to limit 'operators' ability to perform law enforcement functions yet still be protective of the massive amounts of data an LPR system collects.

Because LPR equipment and accounts can have broad permissions, policies should contain language defining what functions an operator can and cannot perform with an assigned LPR account or LPR equipment. Having operators sign an acceptable use statement is a method of tracking and ensuring each user has been made aware of the policies set forth. In addition to the policies already explained, the following specific topics and their relationship to the use of LPRs should also be reflected in policy:

- **Data retention and dissemination** – Data usage policies should conform with jurisdiction laws governing the agencies legal authority to collect, retain, disseminate, and dispose of LPR data. Agencies should have a data retention period in policy (whether it is included in jurisdiction law or not) with justification for the data retention period they choose.
- **Freedom of Information Act (FOIA)** – An agency's FOIA policy should be examined to reflect the legal standards of FOIA.
- **Data security** – Operator passwords, system lockouts, system audits, and user audits should all be addressed in policy. Many of these are already established within an agency or by an overarching governing body. Assurances should be made to maintain compliance with these existing policies.
- **Memorandums of understanding (MOU)** – Many agencies and jurisdictions may decide to work together to establish one large LPR network. This reduces the cost per agency, and the burden of responsibility is shared. An established MOU identifies the roles and responsibilities between the agencies.

See Appendix (C) for Sample LPR Policies from Ohio, Utah, and Virginia.

Training

In addition to having sound policy, formalized training should be in place that conveys the policy content to LPR system operators. Training is a fundamental component of an LPR system. Without properly documented training, operators have no direction for which to properly set up, use, and troubleshoot LPR equipment. Training should emphasize policy (and case law) surrounding data retention. This can serve to assure the public that data are being collected, stored, used, and deleted in a manner consistent with established legal guidelines and policy.



LPR training can be divided into three sections: operations, data analysis, and technical support. All sections of training should be recurring and culminate in a test. This ensures new material is presented and operators remain vigilant in the use of the LPR system.

Operations training should focus on the daily operator of an LPR-equipped vehicle. Like speed-measuring devices, the operator of an LPR-equipped vehicle should be able to set up, operate, and troubleshoot a vehicle-mounted LPR system.

Data analytics could be considered the second most important function of an LPR system.(the most important function being data collection). Having the training necessary to analyze a target vehicle across a network of LPR cameras relies on consistent and thorough training.

The last section of training which that be included in an LPR program is technical support. This section of training encompasses the logistical support staff most agencies will use to up-fit LPR patrol vehicles, monitor fixed sites, perform server maintenance, and perform system upgrades.

LPR Program Staffing

An LPR program should be adequately staffed to provide proper program support, oversight, and planning. Prior to determining staffing levels, a decision should be made if the LPR program will fall under the management and leadership of an existing police hierarchy (such as Operations or Investigations) or if it will be autonomous (specialty unit).

If an agency has fixed LPR equipment in its program, the program should be staffed sufficiently to maintain 24-hour operations to respond to any received alert, such as AMBER Alerts.

An LPR program needs enough employees to install and fix the equipment and employees who can manage both the system and equipment. If agency staffing is limited, employees can effectively multitask and meet the needs of multiple positions at once. If an agency does not have the number of employees or expertise to complete all the required aspects of running an efficient program, contractors can be employed to conduct one or more critical functions of the LPR program.

Equipment

Like staffing, LPR equipment needs to encompass all aspects of the program. A comprehensive, but non-inclusive list of equipment needed for an effective LPR program follows (mobile, fixed, and portable platforms):

MOBILE LPR	FIXED-SITE LPR	PORTABLE PLATFORM
Vehicle-mounted readers	Overhead or pole-mounted readers	Platform: commonly a trailer
Connecting wires from readers to trunk box	Continuous power supply	Continuous power supply (solar combined with battery)
Trunk box	Cellular or fiberoptic network	Cellular network
Mobile systems software	Systems software	Systems software
Mobile computer capable of operating mobile systems software		
GPS-capable antenna		



Vehicle-mounted reader.



Pole-mounted reader.



Trailer-mounted reader.



Roof-mounted LPR.



Trunk-mounted LPR.

There are many LPR manufacturers that produce reliable and durable LPR equipment. Purchasing agents need to consider the proprietary nature of LPR equipment and be aware that some products are not interoperable with others. It is critical for LPR data to properly communicate from the point of collection

(reader) to a central computer (server). LPR data must be securely protected and accessible by operators, most commonly from a desktop- or vehicle-based computer system. Legal considerations need to be addressed before purchasing equipment. For example, a cloud-based data storage system may not be compliant with a jurisdiction's data storage laws.

The specific type of LPR equipment chosen should be driven by agency mission and priorities. Whereas some agencies may prefer only mobile LPR, others may also use fixed-site LPR's, covert equipment, or portable platforms to create a robust LPR program.

When selecting LPR equipment, anticipate and plan for program expansions and logistical support needs. Items such as spare parts, storage facilities, and ancillary equipment should be considered as well.

Summary

A well-thought-out and well-executed LPR program provides law enforcement an additional tool in providing essential public safety services. Establishing an LPR program is a task that should be completed with careful consideration, planning, and organization.

Chapter 7 License Plate Reader Success Stories

Introduction

What follows are documented examples of how License Plate Reader (LPR) technology has benefited law enforcement in the performance of their public safety mission.

On **January 7, 2021**, Kristin Walker from Alabama was putting fuel into her vehicle with her two children in the backseat when a subject jumped into the driver seat to steal the vehicle. Walker was able to remove her children from the vehicle before it was highjacked. With the use of LPR technology, the Rankin County, Mississippi, Sheriff's Office was able to spot the vehicle a short time later and arrest the two subjects involved.

In **December 2020**, a North Carolina DMV License & Theft Bureau Law Enforcement Agent observed a Volkswagen traveling in a toll lane at a high rate of speed and attempted to stop the vehicle. The vehicle operator failed to stop, and with speeds near 130 mph, the pursuit was called off. LPR information was obtained from the North Carolina Turnpike Authority that included photographs of the driver, vehicle, and license plate information. The violator was located, apprehended, and charged with several serious traffic violations.

On **December 19, 2019**, A Delaware guidance counselor allegedly sexually assaulted a minor teenage boy while in Ocean City, Maryland. The victim alleged Allen Reese drove him from Delaware into Ocean City, where he sexually assaulted him. Using Ocean City's LPR, detectives were able to confirm that Reese's vehicle crossed the Route 90 bridge as well as entry and exit times consistent with the dates and times of the assault provided by the victim. Based on the evidence from the victim corroborated by the LPR system, detectives scheduled an interview with the suspect to execute a warrant and collect DNA samples. However, detectives were notified by Homeland Security that a flight to Casablanca, Morocco, had been booked for Mr. Reese. Because it appeared that he was preparing to flee the country to avoid the sexual assault charges, a warrant was immediately issued for Mr. Reese. He was quickly located and held without bond on charges of sexual abusing a minor and third-degree sexual offense.

In **August 2019**, police with Duck, North Carolina, Police Department (an Outer Banks Island community) deployed their LPR systems to find residents who stayed on the island during a mandatory evacuation during Hurricane Dorian. LPR cameras recorded the plate numbers of vehicles exiting the island to determine which registered vehicles did not leave. The homes associated with those vehicles were visited by police to warn those residents of the risks of remaining on the island.

On **July 24, 2019**, a woman put her dog Happy into her car in Baltimore's Guilford neighborhood. She was just getting into the driver's seat when she was forcibly pulled her from her car and several suspects got into her car and sped off. Happy was still in the car when the suspects fled. The woman notified police, and the Baltimore Police Department immediately placed the license plate on an LPR hotlist as a carjacked vehicle. Soon after a patrol officer passed by the vehicle, which

was parked and unoccupied, and received an alarm on the LPR system he was operating. He approached the car and saw that Happy was still inside with the windows closed and doors locked. Because it was a hot July day, the officer smashed a window and rescued Happy before he was overcome from the heat. The woman and Happy were soon reunited.

On **July 15, 2020**, a man shot and killed his ex-girlfriend in the parking lot of her workplace in Springfield, Tennessee. Two days later, the suspect drove through Mt. Juliet, where a Mt. Juliet Police Department (MJPD) vehicle equipped with an LPR system detected the suspect vehicle license plate, alerting the officers who arrested the suspect.

According to MJPD Chief James Hambrick, "It's amazing the stuff that you wouldn't know travels through your city … is actually traveling through your city." That's one of many success stories to come out of the MJPD's use of LPR, Chief Hambrick said.

On **June 30, 2018**, a subject in Sacramento, California, was attempting to cross a street in his wheelchair and was hit and killed by a passing motorist who failed to stop and render aid. The license plate belonging to the vehicle that left the scene was detected by LPR, and the driver was arrested for felony hit and run.

On **March 15, 2018**, James Allen Hayes plead guilty in federal court to committing multiple bank robberies over the course of five months throughout California. Hayes was apprehended as a result of LPR detecting his vehicle traveling between robbery locations.

Robert Sheets was accused of shooting a man on **August 13, 2017**, in Manor Township, Pennsylvania. Sheets returned to the suspect the next day and discovered him still alive. He then shot the victim again, leaving him for dead and fleeing the area. Miraculously, the victim survived and was able to identify the man who tried to kill him as Sheets. The vehicle driven by Sheets was immediately filed in National Crime Information Center as a felony vehicle, which resulted in a hotlist entry on LPR systems across the U.S.

A few days later, in Fairfax County, Virginia, an LPR alerted officers that Sheets was connected to a 2007 Ford Edge heading west on I-66. Fairfax police cruisers pulled in behind Sheets, and after a 38-mile pursuit, Sheets was apprehended.

On **August 26, 2015**, a gunman shot and killed a news anchor and cameraman from a local news station (Alison Parker and Adam Ward) while they were doing a report in Roanoke, Virginia. The license plate number of the shooter was broadcast statewide. Several Virginia State Police patrol vehicles were equipped with LPR. Five hours later and approximately 200 miles away from the shooting scene, Virginia State Police Trooper Pam Neff entered the license plate number into her LPR and discovered the LPR had just read the suspect license plate three minutes prior. Trooper Neff was able to catch up to the suspect vehicle and when back-up was in position proceeded with the apprehension. Trooper Neff was recognized by AAMVA during the AAMVA Annual International Conference in Williamsburg, Virginia, in August 2016.

For more news stories about law enforcement LPR successes from September 2017 to September, 2018, go to https://www.theiacp.org/sites/default/files/ALPR%20Success%20News%20Stories%202018.pdf

Appendix A Significant License Plate Reader Court Cases and Applicable Federal Statutes

United States Court of Appeals for the Ninth Circuit
United States v. Jay Yang,
958 F.3d 851 (9th Cir. 2020).
May 4, 2020
https://law.justia.com/cases/federal/appellate-courts/ca9/18-10341/18-10341-2020-05-04.html

Jay Yang was observed stealing mail from U.S. mail collection boxes on surveillance cameras driving a rented GMC vehicle beyond the rental contract due date. The license plate number was observed and searched in a License Plate Reader (LPR) database, which helped lead investigators to his home. Yang claimed because his rental agreement was past due and the contract was no longer valid when the plate was observed by LPR, the LPR data were invalid, and anything obtained from the search of his residence was not admissible. The court ruled there is no expectation of privacy of a license plate regardless if rental contract was expired. The LPR database did not reveal all the defendant's movements and therefore did not infringe on reasonable expectation of privacy.

United States Court of Appeals for the Eleventh Circuit
United States v. Larry Lamar Wilcox,
415 F. App'x 990 (11th Cir. 2011).
February 28, 2011
https://law.justia.com/cases/federal/appellate-courts/ca11/10-13031/201013031-2011-02-28.html

Larry Wilcox argued the use of LPR technology amounted to unconstitutional surveillance violating his reasonable expectation of privacy. The defendant said the district court erred in denying a motion to suppress, stating an Atlanta police officer's use of LPR technology violated his Fourth Amendment right to be free from an unreasonable search.

The Court of Appeals ruled that the Supreme Court had concluded in similar contexts visual surveillance of vehicles in plain view does not constitute an unreasonable search for Fourth Amendment purposes. Given the Supreme Court's Fourth Amendment precedent, the Court of Appeals ruled the district court did not commit plain error in concluding Wilcox did not have a reasonable expectation of privacy in the plainly visible license plate and the officers' use of LPR did not violate the Fourth Amendment.

United States Supreme Court
United States v. Knotts,
460 U.S. 276, 103 S.Ct. 1081, 75 L.Ed.2d 55 (U.S. 1983).
December 1983
https://supreme.justia.com/cases/federal/us/460/276/

Tristian Armstrong was being investigated for stealing chemicals to manufacture illegal drugs. Agents attached a radio transmitter to a container of chemical sold to Armstrong, which tracked the location of where methamphetamine was being produced by Leroy Knotts. A search warrant was obtained, and an illegal drug manufacturing lab was discovered.

Knotts was convicted in district court, but the U.S. Court of Appeals reversed the conviction, stating Knotts' Fourth Amendment rights were violated by use of the tracking device, and the evidence could be suppressed. The U.S. Supreme Court held the initial conviction, ruling the tracking device did not invade any legitimate expectation of privacy and was neither a "search" nor a

"seizure" by grounds of the Fourth Amendment. The movement of a person traveling on a public highway does not afford an expectation of privacy of the movements. Nothing indicated the tracking device was used to gather information from within the private area.

Privacy and Fourth Amendment

Authority for Police to Check License Plates
United States Court of Appeals for Ninth Circuit
***United States v. Ismael Diaz-Castaneda*,**
494 F.3d 1146 (9th Cir. 2007).
July 18, 2007
https://caselaw.findlaw.com/us-9th-circuit/1468527.html

An officer ran the license plate on a pickup traveling in front of him in traffic. The plate information response indicated that the driver's license of the registered vehicle owner, Solia Diaz, was suspended. The officer, believing the operator fit the description of Diaz, stopped the vehicle. Diaz was arrested for driving while under suspension. The vehicle passenger, Ismael Diaz-Castaneda, was found to have an immigration detainer on him and was arrested.

Diaz-Castaneda argued the stop violated his Fourth Amendment rights, and any subsequent evidence should be withheld. The court held a license plate check does not constitute a Fourth Amendment search, and evidence should not be suppressed.

U.S. Court of Appeals for Sixth Circuit
United States v. Curtis Ellison,
462 F. 557 (6th Cir. 2006).
September 5, 2006
https://caselaw.findlaw.com/us-6th-circuit/1031532.html

A Farmington Hills, Michigan, police officer ran a license plate of a parked vehicle through a police telecommunication system belonging on a vehicle operated by Curtis Ellison. Information returned revealed the registered owner was a "wanted person." Ellison was determined to be a passenger in the vehicle and was arrested. District court originally ruled the officer did not have probable cause to run the plate because the van was not parked illegally, and therefore Ellison Fourth Amendment Rights were violated. The court determined what a person exposes publicly is not subject to Fourth Amendment protection, and observing a license plate displayed in plain view does not constitute a search.

Validity of License Plate Reader Technology

United States Court of Appeals for the Third District
***United States v. Marcus White*,**
504 F. App'x 168 (3d Cir. 2012).
November 15, 2012
https://law.justia.com/cases/federal/appellate-courts/ca3/11-4035/11-4035-2015-04-29.html

Marcus White was convicted in Pennsylvania for his involvement in robberies of a post office and convenience stores. White's vehicle had been reported stolen and was detected by a Maryland state police trooper by an alert from an LPR while on patrol. During the suppression hearing, the District Court noted "the technology used by the license [plate] reader is verifiable and acceptable technology." White did not challenge this conclusion.

Use of License Plate Reader Data

Supreme Court of Virginia
Opinion of Justice Stephen R. McCullough
Harrison Neal v. Fairfax County Police Department, ET AL,
299 Va. 253, 849 S.E.2d 123 (Va. 2020).
October 22, 2020
https://law.justia.com/cases/virginia/supreme-court/2020/191127.html

In a prior ruling, the Virginia Court of Appeals ruled the "passive use" of LPR data by Fairfax County, Virginia, police violated the Virginia Data Act. Neal

argued the police department could not collect and store passively obtained LPR data without suspicion of criminal activity. Neal claimed the Virginia Data Act prohibited the gathering of personal information unless justified by law. The court initially ruled the LPR data provided a link to identify the vehicle owner and therefore LPR data was subject to the Virginia Data Act.

In a later ruling from the Virginia Supreme Court, the court stated the LPR system did not qualify as an information system because it did not contain name, personal number, or other identifying particulars of data for a subject. The court further stated the plate, vehicle photo, date, time, and GPS location did not bring the Data Act into play because the LPR system did not contain all the components and operations of a record keeping process. The court found the police department's passive use of the LPR system was legal.

Massachusetts Supreme Court
***Commonwealth of Massachusetts v. McCarthy*,**
484 Mass. 493, 142 N.E.3d 1090 (Mass. April 16, 2020).
https://law.justia.com/cases/massachusetts/supreme-court/2020/sjc-12750.html

Law enforcement officers were investigating Jason McCarthy's suspected illegal drug activity and deployed LPRs on bridges to track his activity. Police used data from the LPRs and received real-time alerts, which led to the arrest of McCarthy. McCarthy filed motion to suppress the LPR data because it violated his constitutional right to privacy of his public movements. The court ruled the defendant's privacy was not violated because of the limited extent and use of the LPR data.

Reasonable Suspicion for Vehicle Stop Based on License Plate Reader Information

United States Court of Appeals for the Ninth Circuit
***Denise Green v. City and County of San Francisco*,**
751 F.3d 1039 (9th Cir. 2014).
May 12, 2014
https://caselaw.findlaw.com/us-9th-circuit/1666208.html

An LPR operated by a San Francisco Police officer indicated a license plate displayed on Denise Green's vehicle was on a stolen vehicle. A high-risk felony stop occurred, and Green was held at gunpoint, handcuffed, and detained. Eventually, officers ran the actual plate to confirm stolen and determined the LPR misread the plate, and the vehicle was not stolen; Green was released.

San Francisco Police Department officers are trained that an LPR hit does not automatically justify a vehicle stop. Officers are directed to verify validity of the identified hit before executing a stop. Officers are instructed to verify the plate being read by the LPR is truly the plate on the vehicle and to confirm the stol-en "hit" with their police telecommunications system. **The court ruled an unconfirmed LPR "hit" does not form a reasonable suspicion to support an investigatory detention of subject.**

Georgia Court of Appeals
***Hernandez-Lopez v. The State of Georgia*,**
319 Ga. App. 662, 738 S.E.2d 116 (Ga. Ct. App. 2013).
February 5, 2013
https://caselaw.findlaw.com/ga-court-of-appeals/1622591.html

An LPR in use by an officer with the Gwinnett County, Georgia, Police Department indicated a plate belonged to a "wanted person" by the name of Eloy

Hernandez-Lopez. The officer noted a warrant was for an adult male, which matched the warrant identifying information. The vehicle was stopped and the subject operating the vehicle was determined to be Salomon Hernandez-Lopez, and he was arrested for operating without a license.

Hernandez-Lopez claimed the officer lacked reasonable suspicion to conduct a traffic stop based on the LPR information. The court held the officer did in fact have reasonable suspicion based on the LPR information indicating the license plate belonged to a "wanted person." This would be the same as if an officer ran the license plate through the Georgia police telecommunications system directly. **The court ruled an LPR "hit" provides an officer with reasonable suspicion to justify an investigatory stop.**

New York Supreme Court
***People of the State of New York v. Luis Davila, Jr.*, 27 Misc.3d 921, 901 N.Y.S.2d 787 (N.Y. Sup. Ct. 2010), *aff'd*, 137 A.D.3d 655, 26 N.Y.S.3d 862 (N.Y. App. Div. 2016).**
April 1, 2010
https://law.justia.com/cases/new-york/other-courts/2010/2010-20111.html

A New York Police Department LPR mounted on a police vehicle alerted officers to a suspended plate, and the vehicle was stopped. An officer observed what appeared to be a weapon in possession of a vehicle occupant and subsequently arrested the subject for possession of a firearm. Davila contested the arrest, arguing the officer failed to follow department policy by first verifying the LPR data had been updated in the past 24 hours and did not verify the information against the department database. The court ruled the department policies are guidelines and not required by law; therefore, use of LPR to detect the vehicles registration as suspended was lawful.

Related Federal Statutes

28CFR Part 23 Criminal Intelligence Systems Operating Policies
28 CFR Part 23 contains policy standards for law enforcement agencies operating federally funded multijurisdictional criminal intelligence systems. The standards specifically provide guidance for the submission, entry, security, inquiry, dissemination, review, and purge of criminal intelligence information.

2 CFR § 200.79 Personally Identifiable Information (PII).
LPR information is NOT PII
PII is information considered capable of identifying an individual either by itself or with other identifying information. LPR systems contain information consisting of vehicle license plates, vehicle photos, dates, times, and GPS locations—information generally not considered PII. Therefore, LPR information may not be restricted by statutes concerning maintaining PII but can become PII if additional information is included that is defined as PII. Case-by-case assessment is recommended when developing LPR system data maintenance and use.

Driver's Privacy Protection Act (DPPA) of 1994, 18 U.S.C. 2721
The Driver's Privacy Protection Act (DPPA), 18 U.S.C.A. §§ 2721-25 also supports the premise that a license plate number alone is not PII. Enacted in 1994, the DPPA is a federal law that regulates how state motor vehicle departments release information contained in their records. DPPA addresses the prohibition on release and use of certain personal information from state motor vehicle records. Collected LPR information contains no PII that may be used to connect a license plate detection to an individual. It is only with permissible purpose law enforcement may make this connection (using motor vehicle records).

Appendix B Additional License Plate Reader Resources

American Association of Motor Vehicles (AAMVA)

AAMVA – Best Practices and Model Legislation

- License Plate Standard, Edition 2 (2020)

AAMVA – AAMVA Policy Positions

- Alternative License Plates Policy Statement (Adopted 2020)
- License Plates Policy Statement (Amended 2020)
- License Plates Should Not Be Obscured Policy Statement (Amended 2020)
- Temporary License Plates Policy Statement (Amended 2020)

International Association of Chiefs of Police (IACP)

You must be an IACP member with log-in credentials to access these resources:

https://www.theiacp.org/resources/policy-center-resource/license-plate-readers

- IACP License Plate Reader Model Policy (2010)
- IACP License Plate Reader Concepts and Issues Paper (2010)

These IACP resources are publicly accessible:

https://www.theiacp.org/projects/automated-license-plate-recognition

- IACP License Plate Reader Privacy Impact Assessment (2009)
- IACP License Plate Reader Policy & Operational Guidance (2012)
- IACP Resolution: Retro-Reflective Front and Rear Plates (2018)
- IACP Resolution: Digital License Plates (2020)
- IACP Technology Policy Framework (2014)

Police Executive Research Forum

Free Online Documents (policeforum.org)

- Combating Auto Theft in Arizona: A Randomized Experiment with License Plate Recognition Technology: Police Executive Research Forum, December 2011

RAND Corporation

https://www.rand.org/pubs/research_reports/RR467.html

- License Plate Readers for Law Enforcement – Opportunities and Obstacles (2014)

Appendix C Sample License Plate Reader Policies

Introduction

The core business values that License Plate Reader (LPR) promises can only be achieved through proper planning, implementation, training, deployment, use, and management of the technology and the information it provides. Like all tools and technologies available to law enforcement, LPR must also be carefully managed. Agencies must clearly articulate their strategic goals and tactical objectives for the technology, and this strategy should be tightly aligned with the broader strategic plans of the agency. Thorough and ongoing training is required to ensure that the technology performs effectively and that users are well versed in the operational policies and procedures defined and enforced by the agency.

Policies must be developed and strictly enforced to ensure the quality of the data, the security of the system, compliance with applicable laws and regulations, and the privacy of information gathered. Building robust auditing requirements into agency policies will help enforce proper use of the system and reassure the public that their privacy interests are recognized and respected.[1]

Three agency sample policies follow:

Ohio State Highway Patrol

Utah Tax Commission, Motor Vehicle Enforcement Division

Virginia State Police

1 IACP ALPR Policy & Operational Guidance (see Appendix B).

OHIO STATE HIGHWAY PATROL POLICY

Summary of Revisions

Revisions are in red, bold, italics throughout.

Purpose

To provide guidelines for the implementation, installation, and use of mobile and stationary Automatic Plate Reader (APR) technology and equipment at selected locations to scan, detect, and identify license plate numbers appears on selected "Hot Lists."

Policy

A. **STATEMENT OF POLICY –** The Ohio State Highway Patrol will utilize APR technology in patrol cars and at stationary locations to accurately identify license plates ***linked to criminal activity and/or commercial motor vehicle administrative violations.***

B. **FUNCTIONALITY AND OPERATION <41.3.9a>**

1. **Installation –** Stationary and mobile scanners will be installed at selected locations and on selected marked and unmarked vehicles. ***GHQ electronic technicians are responsible for maintaining a list of all locations and vehicles equipped with APR technology.***

2. Data Sources for "hits" – All APRs have the ability to match a captured image to two categories of databases: criminal violations and commercial motor vehicle violations. Officers and MCEIs have the ability to match images with one or both types of databases simultaneously.

a. Criminal Databases: Both mobile and stationary APRs can match captured images with LEADS and NCIC entries with an associated license plate (e.g., stolen motor vehicles, felony warrants, missing persons, protection orders, etc.)

b. Commercial Motor Vehicles – Both mobile and stationary APRs can match captured images with the Federal Motor Carrier Safety Administration PRISM database for commercial motor vehicles placed out of service and ones with an "Inspect" or "Possible" score in the Inspection Selection System (ISS).

3. General Operation – The Division's automatic plate readers capture images of numbers and letters resembling license plates and match those captured images to the current "hot list." The "hot list" is the master index of license plates entered in both data sources listed above. The criminal database "hot list" is updated twice daily and the commercial motor vehicle database "hot list" is updated once daily.

4. Units assigned to enforcement vehicles equipped with mobile APR systems shall ***verify the receipt of*** the most recent "Hot List" from the applicable databases at the beginning of each shift.

5. **Probable Cause** – An APR "hit" from the criminal databases shall not be used as probable cause for a traffic stop or enforcement contact. Contact with the vehicle and occupants shall only be made after the "hit" is confirmed through LEADS/NCIC.

6. **Manual Entry by User into "Hot List" Database** – ***The system does not obtain real***

time information from LEADS/NCIC; therefore, there may be situations which require an officer or dispatcher to manually enter a vehicle registration into the database. These situations include, but are not limited to: active Amber Alerts, Ohio Blue Alerts, endangered missing child alerts, endangered missing adult alerts, BOLOs, and other emergency messages/alerts. Manual entry of a plate into the "Hot List" shall only be done with supervisor approval. See User Manual for entry procedures.

A "hit" on a BOLO that is manually-entered into the system shall not be used as probable cause for a traffic stop or enforcement contact.

7. **'O' vs. Zero** – Because of standardized NCIC formats, a letter 'O' and a zero in a license plate number are synonymous in NCIC records. Therefore, the "hot list," NCIC, and the APR read the letter 'O' as a zero. Any plate entry, including any manually entered by an officer or a dispatcher with an 'O' is automatically converted to a zero.

8. **Fixed Point and APR Notification** – When a license plate entered in the "Hot List" is detected by a stationary APR, a notification is automatically sent by the APR system to an OSP dispatch facility equipped to receive the notifications. When a mobile APR detects a "Hot List" entry, the officer receives an audible and visual notification on the in-car MCT.

9. **Case Documentation** – A record of the APR "hit" shall be included in the case/incident report. All "hits" captured by the APR system shall be stored for 30 days and will then be automatically purged. All "hits" will be stored electronically in the ELSAG system. Access to the ELSAG system is limited to authorized personnel only. <41.3.9b,d>

10. **Storage of "Non-Hits"** – All "non-hit" APR captures shall be automatically purged from the system within a 24-hour period. APR captures shall not be collected, stored, or shared with the intent of data mining. Dispatchers assigned to Cleveland and the Statehouse shall query the system for plates older than 24-hours on a quarterly basis to ensure "non-hit" captures are being deleted in accordance with this policy. Troopers assigned APR equipped enforcement vehicles shall perform the same query as part of the semi-annual vehicle inspection. <41.3.9d>

11. **Training –** Dispatchers, sworn officers, electronic technicians, motor carrier enforcement inspectors, and network administrators shall receive appropriate training from qualified OSP staff or vendor representatives prior to using or maintaining the APR equipment. <41.3.9c>

C. **USER MANUALS –** The manufacturer's user manuals, which provide operational procedures for both the Mobile Auto-Detector User and Operations Center Personnel are attached to this policy.

D. **GUIDELINES FOR USE <41.3.9a>**

1. **Stationary APRs**

   a. **Notification** – After receiving a "hit" through LEADS/NCIC, the dispatcher will verify the APR "hit" on the plate matches the image and follow established procedures to check NCIC/LEADS. The dispatcher will then dispatch an officer to intercept the vehicle. Two officers will be dispatched to verify "hits" at the Statehouse Garage. The officer(s) will be notified of the reason for the "hit," that the dispatch is a result of the APR and that the "hit" has been verified through NCIC.

   b. **Verification of Hit** – If, for any reason, the APR "hit" cannot be verified through LEADS/NCIC, the vehicle is not to be stopped based solely on the APR. If the

Ohio State Highway Patrol Policy (continued)

dispatcher cannot read the digital image sufficiently to verify the license plate number and state, an officer may be dispatched to intercept the vehicle, however the intercepting officer must first verify the "hit" through NCIC prior to stopping the vehicle.

c. **Turnpike Gate Personnel** – If an officer is unavailable to immediately intercept a valid "hit," the dispatcher may notify additional personnel to be on the lookout for the suspect vehicle. Ability to identify the vehicle, reason for the "hit," and known direction of travel should all be used to determine whether additional personnel should be notified. If the vehicle is observed, they should be instructed to notify the dispatch facility of the route and direction of travel.

d. Officers and dispatchers should use their discretion based on hazards, proximity of assisting officers, type of "hit," etc.

e. **Cleveland Dispatch Center / Capitol Square Parking Facility**

i. The APR system will be checked by the dispatcher at the beginning of the shift and the information will be logged on the OTIS HP-53 using File 1 – Sub Category "APR."

ii. The Statistical Analysis function will determine if the APR is functioning correctly. The system should indicate a number of plates that have been checked. If there are no plates indicated, the system is not functioning. If the system shows that plates are being scanned, the system is working correctly.

iii. The Statistical Analysis section is found in section 6 of the User's Guide.

2. ***Mobile APRs***

a. Mobile APRs are operational as long as the officer is logged in to the MCT in the vehicle.

b. Officers have the ability to toggle between the Criminal and Commercial databases or they can activate both. If both databases are active, the mobile APR will indicate a "hit" on a violation in either system.

c. Officers must verify the "hit" through LEADS/NCIC prior to stopping the vehicle. If, for any reason, the APR "hit" cannot be verified, the vehicle is not to be stopped based solely on the APR. Officers only need to verify that the plate matches the "hit" in the FMCSA database.

d. Officers and MCEIs should use their discretion based on hazards, proximity of assisting officers, type of "hit," etc.

e. Motor Carrier Enforcement Inspectors may not stop a commercial motor vehicle for the sole purpose of a LEADS/NCIC "hit".

3. **Infrastructure Specialist and Electronic Technicians are responsible for:** <41.3.9b>

a. Equipment and software deployment and installation

b. Coordinating maintenance and repair

c. Coordinating the establishment of parameters for download of NCIC and LEADS

Ohio State Highway Patrol Policy (continued)

data, pick-up radius restrictions, misdemeanor and/or felony warrants.

d. Ensure all captures on stationary and mobile APRs follow the appropriate retention schedule.

4. **Public Affairs -** All media contacts will be coordinated through the Public Affairs Unit, which shall be consulted prior to releasing any information to the news media.

5. **Licensing and Commercial Standards**

   a. LCS units may stop commercial motor vehicles for the purpose of inspection based on hits received from the PRISM file "Hot List."

   b. The reason code LPRI (License Plate Reader Inspection) will be used in ASPEN for all inspections conducted based on a PRISM hit.

UTAH MVED POLICY

Policy
410

Utah Motor Vehicle Enforcement Division
Po icy Manua

Automated License Plate Readers (ALPRs)

410.1 PURPOSE AND SCOPE

ALPR is a computer-based system that utilizes special cameras to capture a color image, as well as an infrared image, of the license plate of a passing vehicle. The infrared image is converted into a text file utilizing Optical Character Recognition (OCR) technology. The text file is automatically compared against an “informational data file” containing information on stolen or wanted vehicles as well as vehicles associated with AMBER alerts, warrant subjects or other criteria. If a match is found, the user is notified of the vehicle “hit” by an audible alert and an associated notation on the user’s computer screen.

ALPR cameras can be mobile (mounted on vehicles) or on fixed positions such as freeway overpasses or traffic signals. ALPR systems mounted on vehicles have all the necessary equipment to scan plates, notify the user of a vehicle hit, and store the plate scan data for uploading into the ALPR server at a later time. ALPR fixed positions transmit plate scan data to the ALPR server as they are scanned and notify a central dispatch, such as a station desk, of any vehicle hit.

ALPR cameras can photograph thousands of plates in a shift. All plate scan data collected from the ALPR cameras are transmitted to an ALPR server. The ALPR server resides within the State of Utah Data Network Center. In addition to software applications that are used to run the ALPR server, the ALPR server also houses the “informational data file” containing wanted, stolen, or vehicles of interest, as well as all the plate scans captured by the ALPR cameras.

The informational data file is comprised of information from the Stolen Vehicle File (SVF), “HOT FILE” (HF), Wanted Persons File (WPF), Stolen Plate File (SPF), Revoked Registration File (RRF), Cancelled Registration File (CRF), Expired Registration File (ERF), Out of Service (OS), and user defined “hot lists.“ The Informational data file is updated throughout the day with different data sources being “refreshed” at different intervals. SVF/WPF/SPF/RRF/ERF/OS data is refreshed from the state database daily, HF data is refreshed from the Bureau of Criminal Investigation hourly, CRF data is refreshed weekly, and hot list data is refreshed upon input into the ALPR server. It is important that ALPR users take into account the amount of lag time between receiving an ALPR hit notification and the last updating of the informational data file within the mobile ALPR unit database. When possible, confirm that the mobile ALPR unit hit information is still valid, either through your Communication Center (CC) or via your laptop computer (LC) prior to taking police action. Confirmation can be deferred in rare circumstances (i.e. special investigative units) when compelling circumstances may exist that, if CC is contacted, it could jeopardize the investigation and/or officer safety.

Fixed ALPR cameras have a continuous connection to the ALPR server. They are capable of uploading plate scan data to the ALPR server as the scans occur. ALPR scans can be compared against the informational data file immediately when the data sources are updated. Mobile ALPR units do not have a continuous connection to the ALPR server. In order to facilitate the exchange of data, air cards are used which will allow connectivity to the ALPR server via wireless transmission.

Copyright Lexipol, LLC 2020/08/26, All Rights Reserved.
Published with permission by Utah Motor Vehicle Enforcement Division

Utah Motor Vehicle Enforcement Division

Po icy Manua

Automated License Plate Readers (ALPRs)

If the air card in the vehicle is connected to a service, the ALPR will continually “sync” which will upload plate scan information from the vehicle to the ALPR server and/or download the latest informational data file from the ALPR server to the vehicle. It is imperative that mobile ALPR users sync their mobile units at least once at the beginning of their shift to ensure they have the latest informational data available.

410.2 POLICY AND PROCEDURES

Mobile ALPR unit users receiving an alert shall confirm the status of the vehicle by running the license plate either manually via the LC or over the radio via CC, unless compelling circumstances are present or officer safety issues make it unsafe to do so.In such cases, Officers shall confirm the status of the alert as soon as possible. When requesting CC to confirm the status of an ALPR alert, the officer shall advise CC the request is for an ALPR alert.

In the case of a stolen vehicle alert, personnel may regard the vehicle as a known stolen vehicle, while awaiting a secondary confirmation. If the decision is made to initiate a “felony stop” due to an ALPR alert on a stolen vehicle, officers shall advise CC they are following a vehicle due to an ALPR stolen vehicle alert prior to receiving a secondary confirmation by LC/CC.

Officers shall adhere to the Department’s pursuit policy as described in the Manual of Policy and Procedures. CC shall immediately provide secondary confirmation or advise the unit that the vehicle is not reported as stolen.

When Desk Personnel receive an alert from a fixed ALPR system, which is the result of an image taken from a fixed camera, they shall confirm the current status of the vehicle via their CAD terminal or via CC. While waiting for confirmation, desk personnel will advise field patrol units of the ALPR alert, the location, the vehicle description, request aero bureau, and coordinate responding field units.

410.2.1 HOT LISTS

Hot lists are comprised of user defined data that is manually input into the informational data file so that ALPR users will be alerted whenever a “vehicle of interest” is located.Hot lists can be loaded into a specific station area vehicle or to ALPR all vehicles countywide.

Hot lists can be input into the ALPR server informational data file only by ALPR administrators. Unit commanders, or their designees, must approve hot list information that is intended for use solely in their area cars. With the exception of AMBER alert information, hot list information intended for Department-wide use must have the approval of the Division Director, or his designee.Mobile ALPR users can input individual license plates into their patrol vehicle’s ALPR system for use during their shift, however, the information will be deleted from that mobile ALPR unit once user performs an “end shift” and the vehicle syncs with the ALPR server. An ALPR vehicle alert identified via hot list information does not automatically provide ALPR users with sufficient justification to pullover or detain vehicle occupants. Often times, these hotlists will identify a “vehicle of interest” which is not necessarily wanted for a crime (ex: sex offender vehicle).

Copyright Lexipol, LLC 2020/08/26, All Rights Reserved.
Published with permission by Utah Motor Vehicle Enforcement Division

Utah MVED Policy (continued)

Personnel must use discretion and in some cases have independent information justifying a traffic stop.

410.3 ALPR OPERATION

Use of an ALPR is restricted to the purposes outlined below. Department personnel shall not use or allow others to use, the equipment or database records for any unauthorized purpose.

(a) An ALPR shall only be used for official and legitimate law enforcement business (Utah Code 41-6a-2003).

(b) An ALPR may be used in conjunction with any routine patrol operation or official investigation. Reasonable suspicion or probable cause is not required before using an ALPR.

(c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

(d) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

(e) If practicable, the investigator should verify an ALPR response through the Utah Department of Public Safety (DPS) law enforcement information system or other appropriate database before taking enforcement action that is based solely upon an ALPR alert.

(f) No ALPR operator may access the DPS database or other system unless otherwise authorized to do so.

410.4 ALPR DATA COLLECTION AND RETENTION

All data and images gathered by an ALPR are for the official use of the Utah Motor Vehicle Enforcement Division and because such data may contain confidential information, it is not open to public review. ALPR information gathered and retained by this department may be used and shared with prosecutors or others only as permitted by law (Utah Code 41-6a-2004).

The Administration Lieutenant is responsible to ensure proper collection and retention of ALPR data, and for transferring ALPR data stored in department vehicles to the department server on a regular basis, not to exceed 30 days between transfers.

All ALPR data downloaded to the server should be stored for the minimum period established by department records retention guidelines and thereafter should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action. In no event shall data be maintained longer than nine months unless it is subject to a warrant, preservation request or disclosure order (Utah Code 41-6a-2004). Data that will not be purged should be downloaded from the server onto portable media and booked into evidence.

Copyright Lexipol, LLC 2020/08/26, All Rights Reserved.
Published with permission by Utah Motor Vehicle Enforcement Division

Utah Motor Vehicle Enforcement Division
Po icy Manua

Automated License Plate Readers (ALPRs)

410.4.1 NON-GOVERNMENTAL AGENCY ALPR
ALPR data captured by a non-governmental agency device may only be obtained pursuant to a warrant or a court order (Utah Code 41-6a-2005).

410.5 ACCOUNTABILITY AND SAFEGUARDS
All saved data will be closely safeguarded and protected by both procedural and technological means. The Utah Motor Vehicle Enforcement Division will observe the following safeguards regarding access to and use of stored data:

(a) All non-law enforcement requests for access to stored ALPR data shall be referred to the Office Manager and processed in accordance with applicable law.

(b) All ALPR data downloaded to the mobile workstation and server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

(c) Persons approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

(d) Such ALPR data may be released to other authorized and verified law enforcement officials and agencies at any time for legitimate law enforcement purposes.

(e) ALPR system audits should be conducted on a regular basis.

Copyright Lexipol, LLC 2020/08/26, All Rights Reserved.
Published with permission by Utah Motor Vehicle Enforcement Division

Virginia State Police Policy

Virginia Department of State Police

General Order OPR 1.20 **License Plate Reader Operating Procedures**

Purpose: To establish uniform guidelines for License Plate Reader operations by Department personnel.

1. The License Plate Reader (LPR) program is intended to enhance law enforcement operations related to homeland security and terrorist watch lists, stolen vehicles and license plates, sex offender violators, wanted and missing persons, and other vehicle-related crimes that impact the safety of citizens.

2. The Director of the Bureau of Field Operations (BFO) shall appoint a Statewide LPR Program Coordinator who shall be responsible for the daily operations of the LPR Program.

Guidelines for Use

3. The Department's LPR system shall be used for official law enforcement purposes only. No employee may use, or authorize the use of, the equipment or database records for any other reason. Misuse of equipment or database records may result in disciplinary action.

4. LPR units will be installed in Department vehicles as determined by the Director of BFO or his/her designee. The Director of BFO must pre-approve the transfer of an LPR unit to another Area. Otherwise, if a sworn employee assigned a vehicle equipped with an LPR unit is transferred, promoted or resigns, the vehicle will be reassigned to another sworn employee and retained in the original Area.

5. LPR-equipped vehicles may be used for routine patrol or during special events. In all instances, LPR-equipped vehicles shall be operated in accordance with Department policies regarding vehicle operations.

6. Each employee assigned an LPR unit is responsible for ensuring they are operating with the most current "Hotlist" at the beginning of each shift. The Statewide LPR Program Coordinator should be contacted immediately if problems are encountered with the updating of the LPR units.

7. Upon receiving an alarm or hit, the sworn employee shall verify the accuracy of the information by contacting the Communications Center per established Department policy.

Effective Date – 10/1/2018 Review Date – 7/1/2022
BFO

General Order OPR 1.20

a. An LPR alarm alone is NOT sufficient probable cause to warrant a stop or arrest.

b. Sworn employees are required to confirm a positive hit prior to any enforcement action being taken.

8. Sworn employees are required to ensure that all positive hits on the Terrorist Watch List are reported to the Terrorist Screening Center (TSC) and Virginia Fusion Center (VFC) immediately. All Terrorist Watch List hits will be handled by MDT or telephone. There will be no radio traffic concerning terrorist hits except in the case of emergencies.

9. Special circumstances, such as AMBER Alerts or critical incidents, may require immediate manual updating of the LPR system "hot list." Sworn employees in possession of license plate information related to such circumstances will immediately enter the data into the LPR system. The Virginia Fusion Center (between 0600 and 2200 hours) and/or Statewide LPR Program Coordinator will ensure that new information is uploaded or relayed to all active LPR units. If a critical situation requires manual entry of license plate data, the Communications Center shall immediately notify all LPR users of the new data in the Division and document this action in the CAD system. LPR users shall manually enter the license plate information associated with the critical incident. The Communications Center shall also contact the Virginia Fusion Center and provide the information so that the data may be entered into the statewide list.

10. Terrorist organizations have openly voiced their desire to attack venues where large crowds gather, such as major sporting events, large festivals, etc. Because of the potential of just such an incident, stationary, mobile, and covert LPR use is permitted for such events. Prior to utilizing LPRs at these venues, the affected Division Commander shall submit a letter, through channels, to the Superintendent describing the event, potential threat, and parameters under which the LPRs will be utilized. The decision to grant the approval rests with the Superintendent's Office.

11. Fixed and/or covert LPR units may be used to support on-going criminal investigations or approved venues. The use of fixed and/or covert LPR units shall be coordinated with the Statewide LPR Program Coordinator.

12. At the end of each month, Monthly Plate Reader Activity Logs will be submitted to the appropriate Area Office and Division LPR Coordinator by personnel using an LPR unit.

General Order OPR 1.20

a. At the Area office, a separate file will be maintained for each LPR unit assigned to the Area. Each file will include all Monthly Plate Reader Activity Logs submitted after LPR system usage. These logs will be handled as Department-governed non-records (DGNRs) and shall be retained for two years after the end of the calendar year.

b. At the Division headquarters, all Monthly Plate Reader Activity Logs will be reviewed by the Division LPR Coordinator and consolidated into one Monthly Plate Reader Activity Report. The report shall be reviewed by the Division Commander and forwarded to the Statewide LPR Program Coordinator by the 5th of each month. The Division is the record holder for the Monthly Plate Reader Activity Reports, and these reports shall be included on the Division's file list. Monthly Plate Reader Activity Reports shall be retained for two years after the end of the calendar year.

Data Security and Access

13. The Statewide LPR Program Coordinator is responsible for overall operations of the program, including:

    a. controlling access of sworn personnel to the LPR system and hot file data;

    b. ensuring stored data are purged from the LPR system server as required;

    c. approving or denying in writing requests to access and/or use LPR data; and,

    d. designating personnel who will be authorized to access the server and conduct data queries.

14. The Department's Data Center will house the Department's LPR System Operations Center, which is the central database for all license plates scanned by the Department's LPR units.

    a. All collected data will be maintained on an independent server that is not connected to, or shared with, other law enforcement databases.

    b. The Data Center will provide an inquiry tool, history tracking, and reporting protocols for the entire LPR program.

    c. The Data Center will provide a secure intranet site, allowing only approved personnel password-protected access to collected data. This access shall be restricted to:

(1) searching for a license plate or partial license plate;

(2) viewing the image and location of matches on the "hot list";

(3) viewing maps showing the location of alarms or hits;

(4) viewing statistical reports on alarms or hits; and,

(5) searching for matches for a specific geographical location and/or time frame.

Operator Training

15. All users must receive standardized training prior to operating the LPR system.

a. The Statewide LPR Program Coordinator is responsible for providing initial training of all Department personnel who utilize the LPR system.

b. Additional training will be provided as needed and as determined by the Statewide LPR Program Coordinator.

c. The Training Division will be responsible for maintaining and updated all training records associated with the LPR program.

Data Storage and Retention

16. Per the Virginia Attorney General's Opinion #12-073, "License Plate Readers – Use and Storage of Data," the Department may not passively collect and store plate read data for potential use in future investigations.

a. The collection and use of stored data to help solve future crime are prohibited under the Opinion and existing Virginia law.

b. The Department may continue to use the LPRs to compare active reads to existing lists, such as stolen vehicles or Amber Alerts. Only the reads that are directly related to the intended purpose (i.e., stolen plate) may be retained beyond the use session of the LPR. All other non-relevant, passive reads should be deleted at the end of that day's use.

c. The Department may collect, store, and analyze data that relates to a specific, on-going, active investigation. That data shall be made part of the criminal investigative file and may not be used for other purposes.

d. The Department may collect and temporarily store data that relates to special events as enumerated in paragraphs 10 and 11 of this General Order. This data will only be stored during the event and will be disposed of immediately following the event if it has been determined no applicable criminal investigation has been initiated. If an applicable criminal investigation is initiated, the data will be handled in accordance with paragraph 16.c. of this General Order.

Appendix D AAMVA License Plate Reader Working Group Roster

CHAIR AND LAW ENFORCEMENT REPRESENTATIVE

Captain Matthew Beaudin
Colorado State Patrol

LAW ENFORCEMENT REPRESENTATIVES

First Sergeant Robert Alessi
Virginia State Police

Lieutenant Chris LaPrairie
Nevada Highway Patrol

Captain Joseph Moody
North Carolina Department of Motor Vehicles
License & Theft Bureau

Colonel Allan Shinney
Utah State Tax Commission

Sergeant Jonathan Zarkauskas
Virginia State Police

MVA REPRESENTATIVES

Betty Johnson
Division Administrator
Nebraska Department of Motor Vehicles

Rosa Yaeger
Director
South Dakota Department of Revenue

IACP REPRESENTATIVE (MEMBER)

Major Josh Swindell
Ohio State Highway Patrol

IACP REPRESENTATIVE (STAFF)

Ryan Daugirda
International Association of Chiefs of Police

TECHNICAL ADVISORS

Dennis Bernardo D'Annunzio
Firmware and Software Development Manager
Leonardo

Jeff Hielsberg
Regional Sales Director
Intellectual Technology, Inc.

Kyle Hoertsch
Vice President of Public Safety Client Relations
Motorola Solutions

Steve Vaughn
Vice President of Field Operations
PrePass Safety Alliance

Mark Muriello
Director, Policy & Government Affairs
International Bridge, Tunnel and Turnpike Association

AAMVA STAFF – PROJECT MANAGER

Brian Ursino
Director, Law Enforcement Programs
American Association of Motor Vehicle Administrators

AAMVA STAFF

Paul Steier
Director, Vehicle Programs
American Association of Motor Vehicle Administrators

1524

OUR VISION

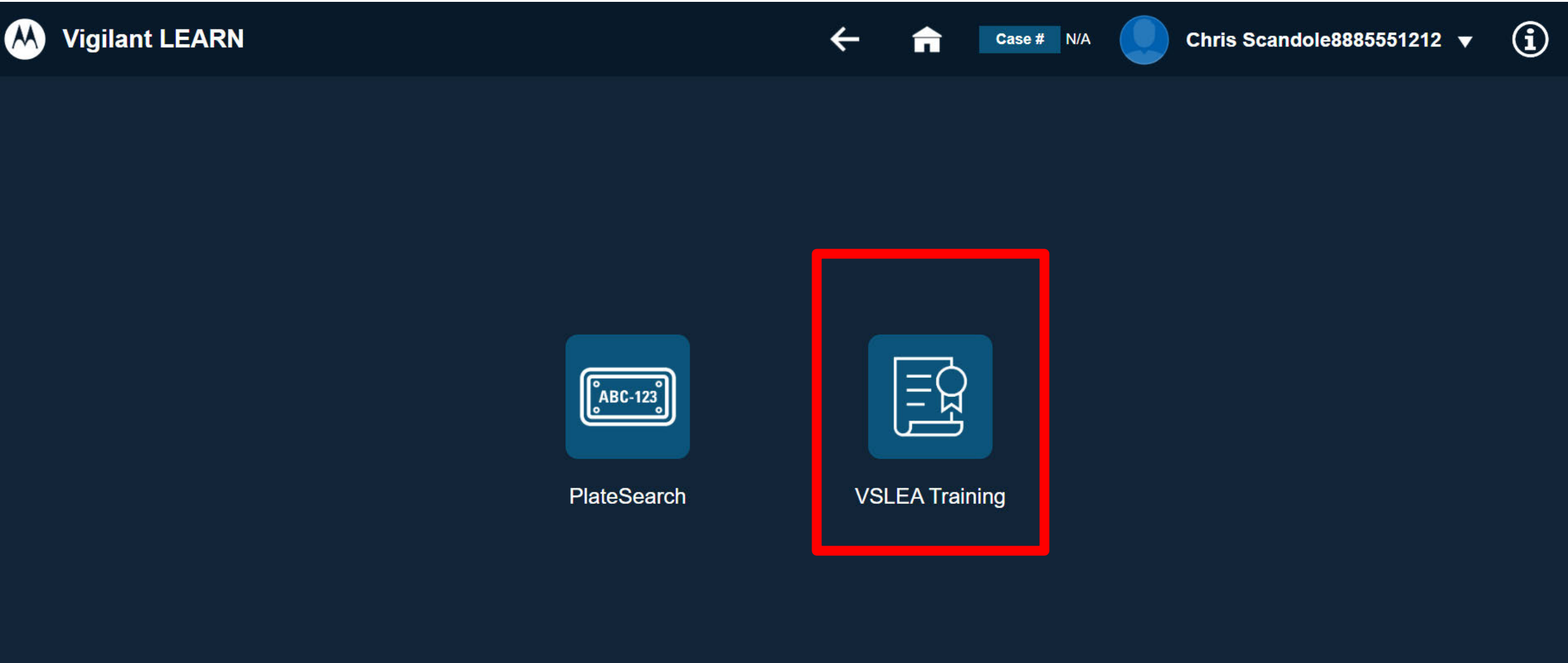
Safe drivers
Safe vehicles
Secure identities
Saving lives!

AAMVA

American Association of Motor Vehicle Administrators
4401 Wilson Blvd, Suite 700
Arlington, Virginia 22203
703.522.4200 | **aamva.org**

1525

WHILE LOGGED INTO LEARN CLICK ON THE VSLEA TRAINING ICON



WHEN YOU ARE RE-DIRECTED TO VSLEA.ORG CLICK ON TRAINING ON-DEMAND

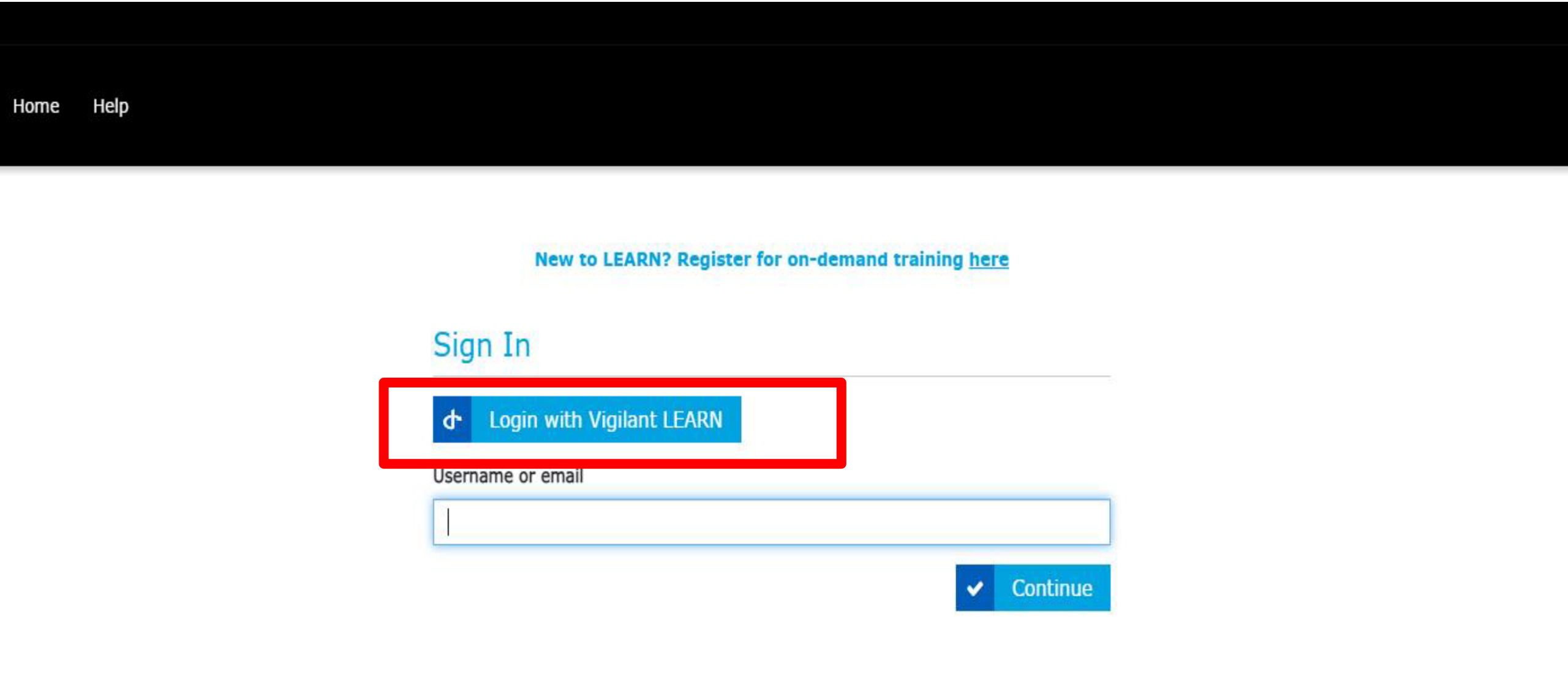


Tags: All, Agency Management, AZ, CA, CT, Facial Rec, FL, IADLEST, IL, Key Skills Webinar, LPR, MS, On-Site, POST, Webinar

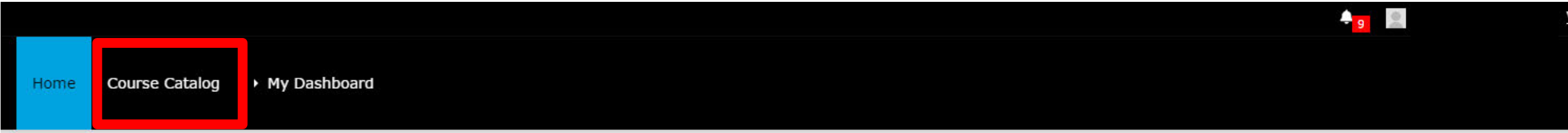
November 2022	December 2022
November 03, 2022 - Thursday **Technical Service Bulletin: Vigilant PlateSearch 7.0.207 Update** Register	December 01, 2022 - Thursday **License Plate Recognition Technology: Basic User** Macclenny, FL Apply For Training
November 07, 2022 - Monday **Technical Service Bulletin: CarDetector Fixed 6.0.199.2 Release** Register	December 06, 2022 - Tuesday **FaceSearch 101 - The Basic** KEY SKILLS WEBINAR Register

1527

WHEN YOU ARE RE-DIRECTED TO POLICE ONE CLICK ON LOGIN WITH VIGILANT LEARN



TO SEE AVAILABLE COURSES CLICK ON COURSE CATALOG



MOTOROLA SOLUTIONS

Vigilant LEARN Training Bulletin:

Welcome to Vigilant Training Academy

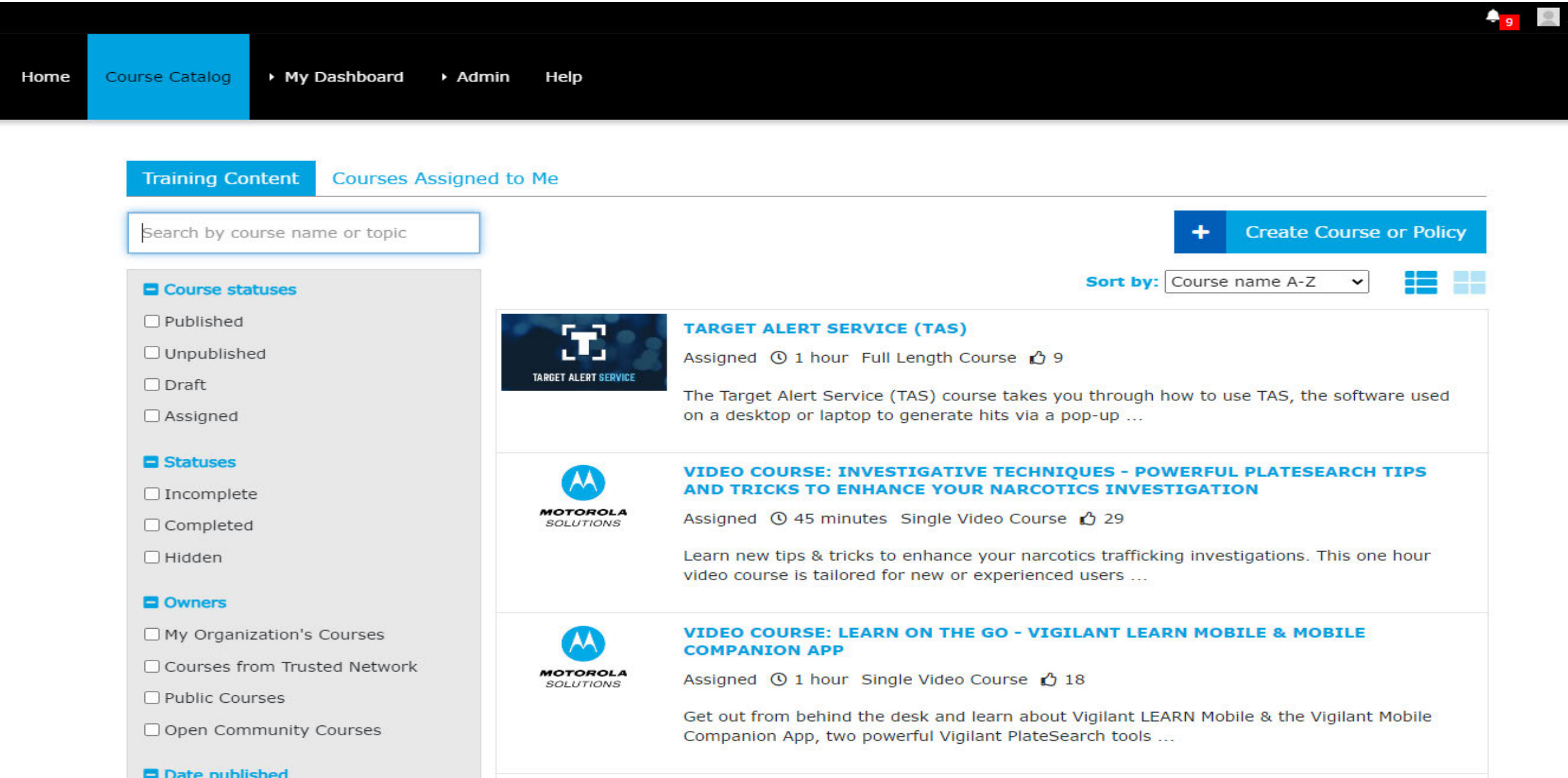
Vigilant Training Academy is an online on-demand learning program to help you learn more about tools that will enhance your investigations. These courses can be completed at your own pace and offer a comprehensive look into how the technologies can be applied into your investigation process.

To get an understanding of Vigilant PlateSearch, begin with the **Vigilant PlateSearch Introduction & User Account Management Course** and work your way through **Vigilant PlateSearch 101** & **Vigilant PlateSearch 202** . You will receive a certificate upon completion of each course.

Other available courses include **Vigilant LEARN Agency Manager** , **Target Alert Service (TAS)** , & **Vigilant CarDetector** . View training manuals and installation guides in the **Vigilant Documentation** area.

Click on **Course Catalog** in the menu bar to view all available courses, documentation , & videos.

CHOOSE WHICH COURSE TO TAKE





CONTACT US

MARCIA BRODERICK
Director, Client Relations - US
(279) 201-4142
marcia.broderick@motorolasolutions.com

DAVID RIVERA
Manager, Client Relations
Southeast Region - US
(813) 460-6993
david.rivera1@motorolasolutions.com

MIKE PRATE
Manager, Client Relations
Northeast Region - US
(934) 500-9658
michael.prate@motorolasolutions.com

CHRIS SCANDOLE
Manager, Client Relations
East Central Region – US
(917) 913-3351
christopher.scandole@motorolasolutions.com

SAM PALMER
Manager, Client Relations
West Region - US
(480) 549-2901
sam.palmer@motorolasolutions.com

LEE YONEMURA
Manager, Client Relations
West Region - US
(916) 307-0893
Lee.yonemura@motorolasolutions.com

VIGILANT TRAINING TEAM EMAIL

VigilantTraining@motorolasolutions.com

Please send us your software update ideas and success stories.

THANK YOU AND STAY SAFE.

VIGILANT VEHICLEMANAGER QUICK GUIDES

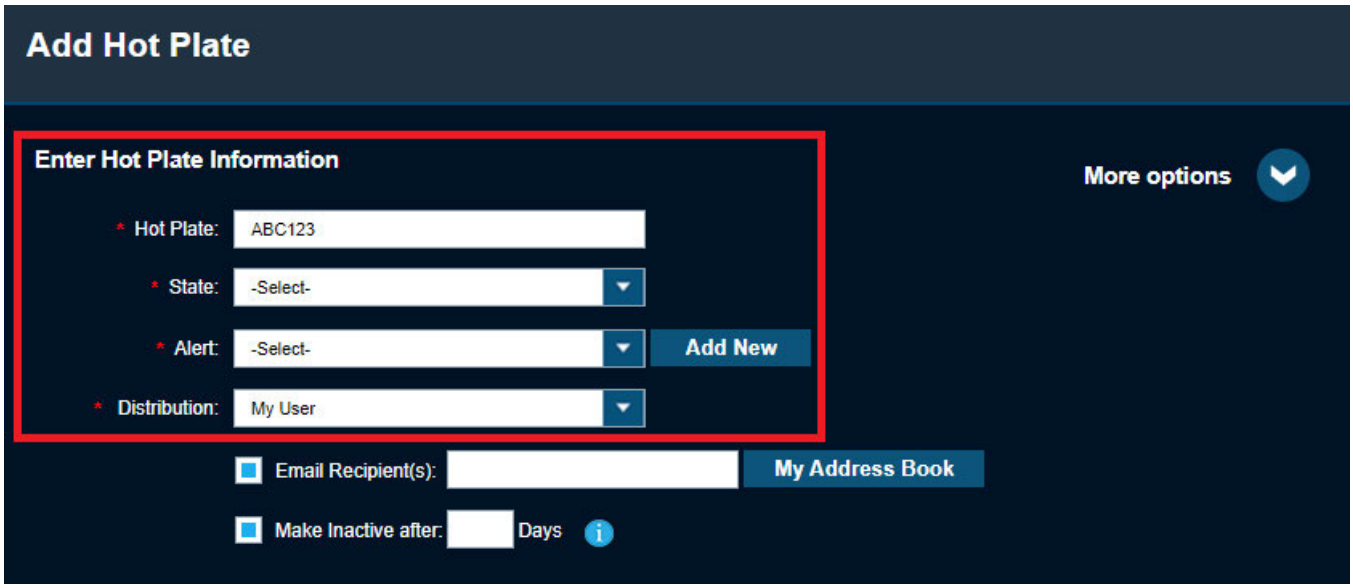
ADDING NEW HOTPLATES

This guide describes how Users and Agency Managers can add new **Hot Plates** to Vigilant VehicleManager and then search for and modify those records.

- **Hot Plates** are license plate records with associated alert and distribution options that generate alerts when detected by Vigilant camera systems.
- **Hot Lists** are lists of **Hot Plates** with alert and distribution options that apply to the entire list.

Hot Plates and **Hot Lists** can be distributed to an entire Agency, individual Users, or to groups of Users that are part of a User Profile.

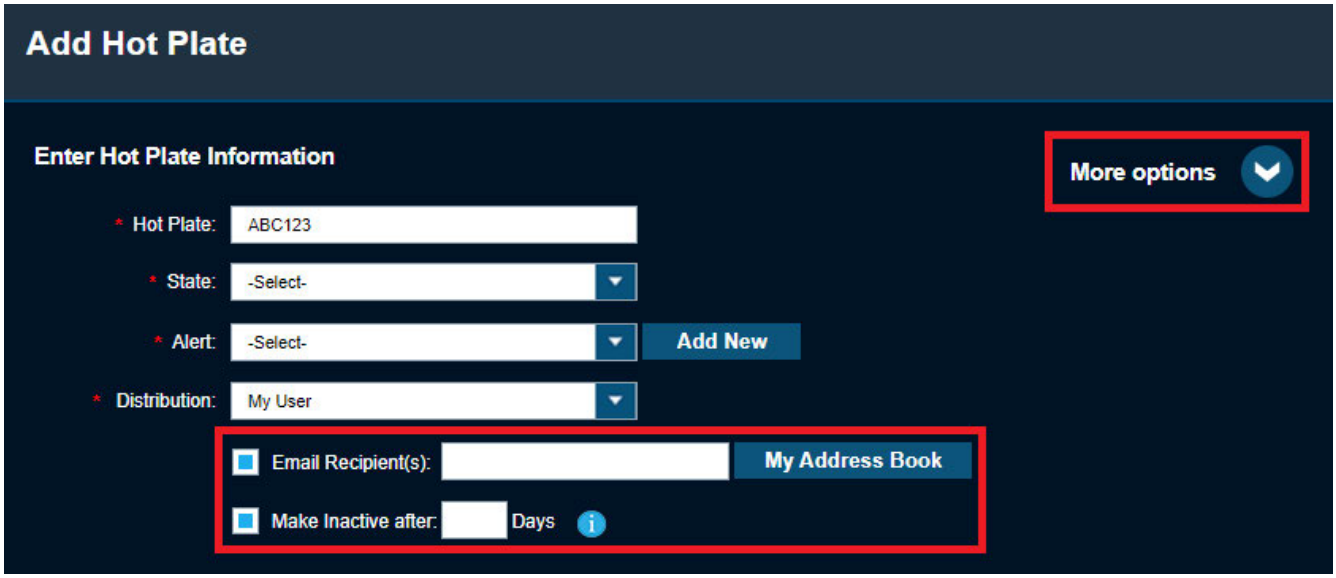
ADDING REQUIRED HOT PLATE INFORMATION



1. Login to Vigilant VehicleManager with an Agency Manager account and navigate to **Hot list management → Upload hot list → Add hot list → Add hot plate.**
2. Enter the following required information:
    a. **Hot Plate:** The alphanumeric license plate number.
    b. **State:** The state or territory in which the license plate is registered.
    c. **Alert:** The alert type that will be generated when the Hot Plate is detected. If desired, use the **Add New** button to add a new Alert type and select it from the drop down list.
    d. **Distribution:** The Users that will receive alerts when this Hot Plate is detected: All Users in the Agency, just this User, selected Users, or certain groups of Users.

© 2023, Motorola Solutions. All rights reserved. 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.

ADDING OPTIONAL HOT PLATE INFORMATION



1. Enable the **Email Recipient(s)** checkbox and enter additional email addresses that will receive the select Alerts when this Hot Plate is detected.

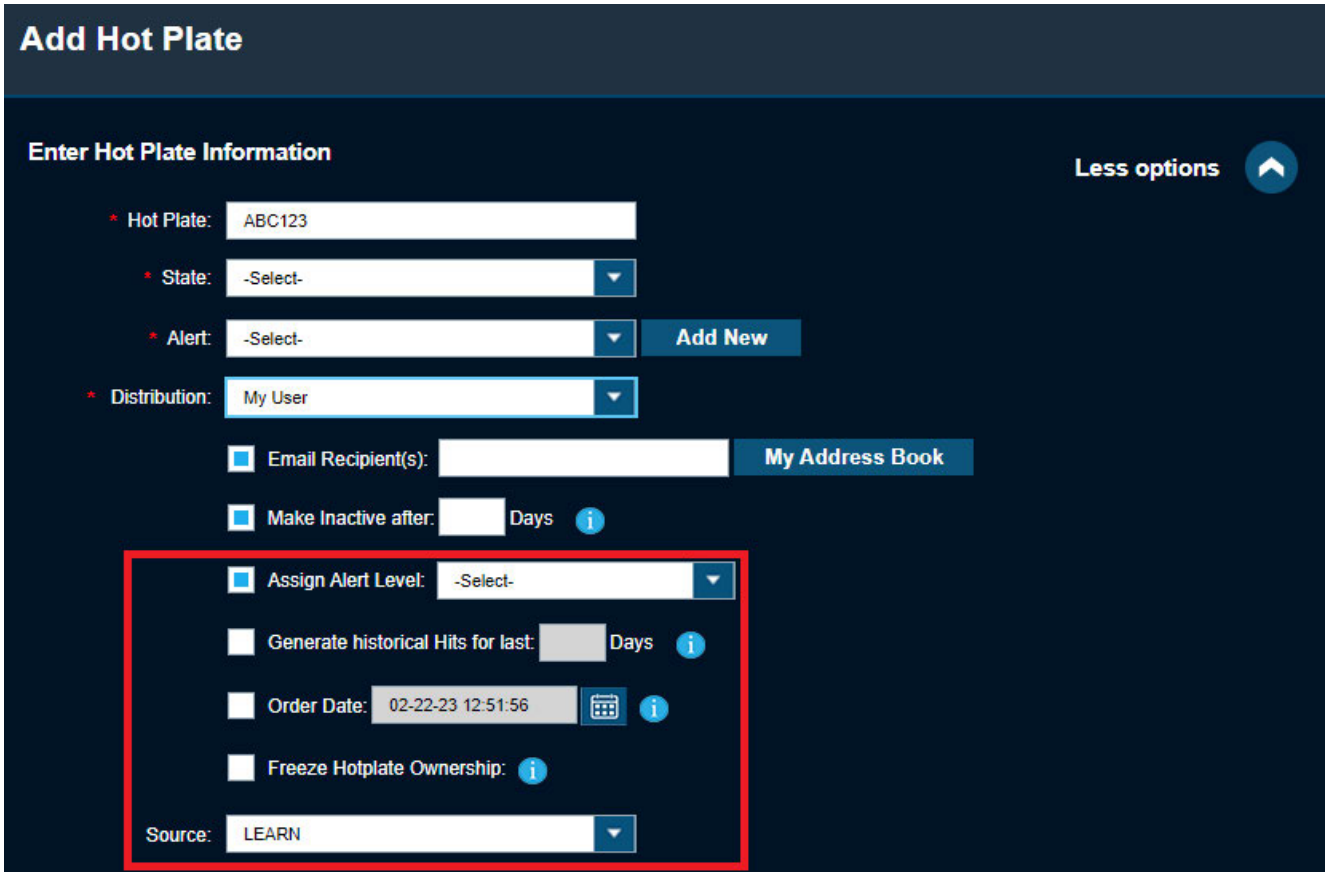
   NOTE: To enter more than one email address, use the **My Address Book** button to add and select additional addresses. Or, use a comma **(,)** to separate each address.

2. Enable **Make Inactive after** to select the number of days after which this Hot Plate record will be inactive and no longer generate alerts.

3. Click **More Options** to open additional Hot Plate configuration options.

© 2023, Motorola Solutions. All rights reserved. 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.

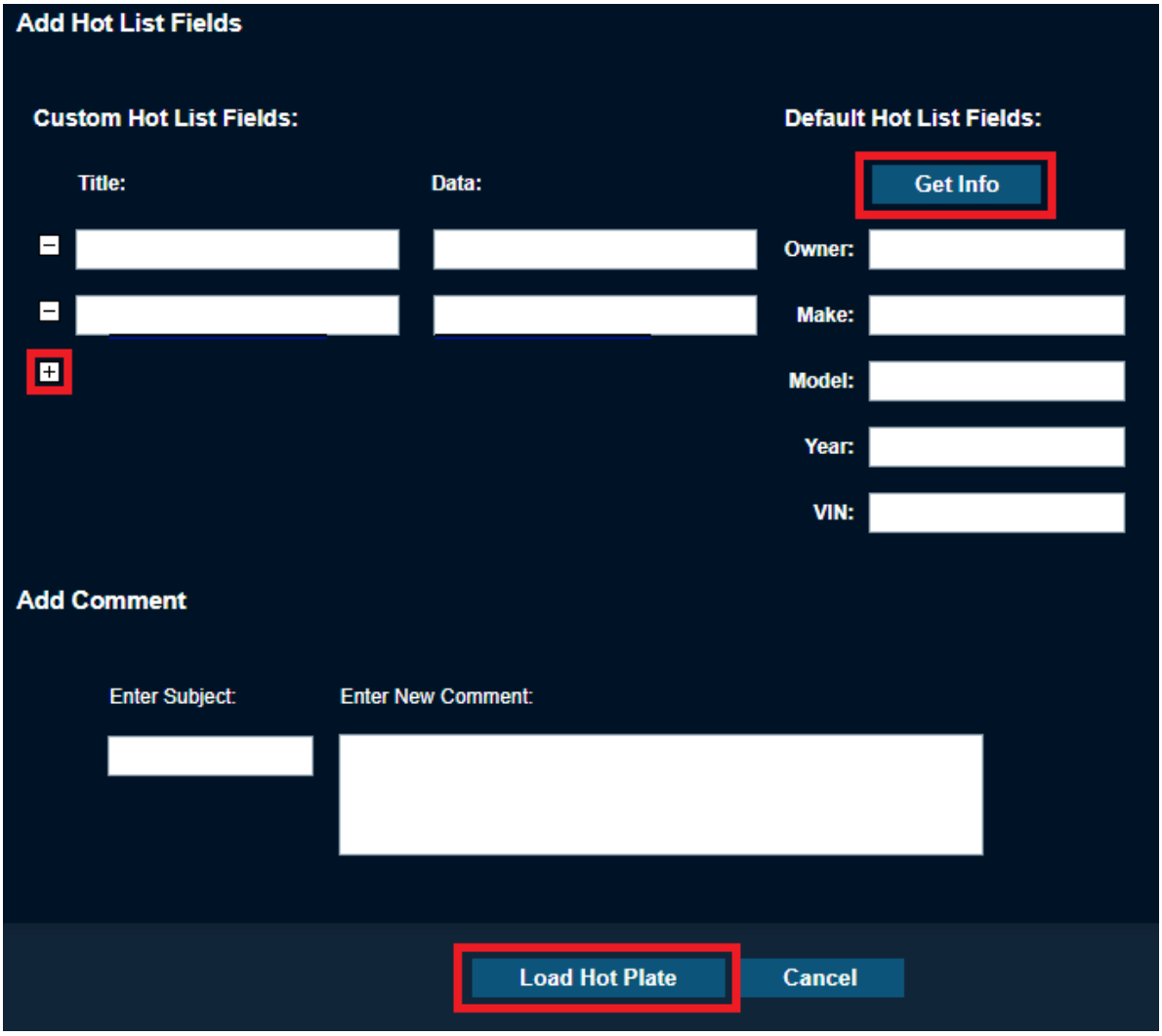
CONFIGURING MORE OPTIONS



1. Select front the following options:
    a. **Assign Alert Level**: Enable to select the urgency of the Alert.
    b. **Generate historical Hits**: Enable and select the number of days to look back and generate Alerts for past detections of this Hot Plate.
    c. **Order Date**: Enable to manually select a different date for the creation of the Hot List record.
    d. **Freeze Hotplate Owner**: Enable to prevent the overwriting of this Hot Plate by another Agency member until the Freeze Ownership option is removed from this record.
    e. **Source**: Select a Source that this Hot Plate will be added to. When that Source is selected by other Users or Agency Managers, this Hot Plate will be active for them.

© 2023, Motorola Solutions. All rights reserved. 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.

ADDING ADDITIONAL HOT LIST FIELDS



2. Enter any additional information about the Hot Plate or vehicle that may be available:

    a. **Custom Hot List Fields**: Enter a type of data in the **Title** field and the data itself in the **Data** field. For example: Windows, Tinted. Use the **Plus Sign (+)** to add additional fields.

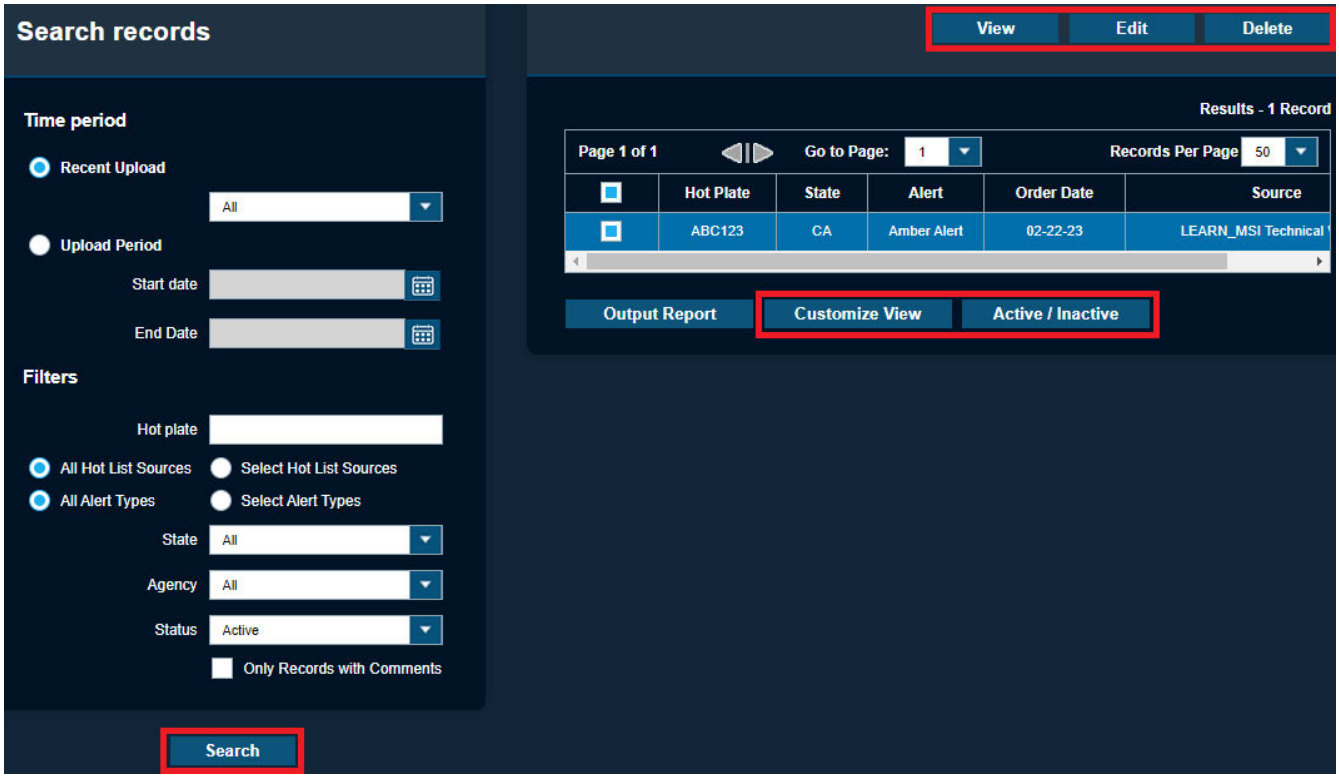
    b. **Default Hot List Fields**: When the **Hot Plate** field is populated, click the **Get Info** to automatically populate the default fields with available data. Enter any additional vehicle information present.

    c. **Add Comment**: Enter a subject and any additional notable information about the Hot Plate record as desired.

3. After all the required and optional information has been entered, click **Load Hot Plate** to create the Hot Plate record.

© 2023, Motorola Solutions. All rights reserved. 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.

SEARCHING FOR HOT PLATE RECORDS



1. To search for Hot Plate records, navigate to **Hot List Management** → **Search Records**.
2. If necessary, select from the **Time Period** and **Filter** options to narrow the search. Click **Search**.
3. In the search results, click on a single Hot Plate to highlight it or use the checkboxes to select multiple Hot plates.
4. Select from the following search result options:
    a. **Customize View**: **Add** or **Remove** fields to display in the search results.
    b. **Active/Inactive**: Inactive Hot Plates are still stored, but will not generate alerts.
    c. **View**: View the Hot Plate records and associated information.
    d. **Edit**: Edit any of the details of an existing Hot Plate record.
    e. **Delete**: Deletes the selected Hot Plate records.

© 2023, Motorola Solutions. All rights reserved. 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.

SUPPORT

For assistance with the topics covered in this guide or with any Vigilant product, please contact the Vigilant Training Team or any of the Client Relations Managers below. **Please send us your software update ideas and success stories!**

CHRIS SCANDOLE
Manager, Client Relations, PS
Central Region – US
(917) 913-3351
christopher.scandole@motorolasolutions.com

LEE YONEMURA
Manager, Client Relations, PS
West Coast – US
(916) 307-0893
lee.yonemura@motorolasolutions.com

DAVID RIVERA
Manager, Client Relations, PS
Southeast Region – US
(813) 460-6993
david.rivera1@motorolasolutions.com

CHRIS PITTMAN
Manager, Client Relations, PS
South Central – US
(469) 712-3060
chris.pittman@motorolasolutions.com

SAM PALMER
Manager, Client Relations, PS
North Central – US
(480) 549-2901
sam.palmer@motorolasolutions.com

MARCIA BRODERICK
Director, Client Relations Nationwide
(279) 201-4142
marcia.broderick@motorolasolutions.com

MIKE PRATE
Manager, Client Relations, PS
Northeast Region – US
(934) 500-9658
michael.prate@motorolasolutions.com

VIGILANT TRAINING TEAM
VigilantTraining@motorolasolutions.com

© 2023, Motorola Solutions. All rights reserved. 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.

TRAINING

For free training, visit VSLEA.ORG



THANK YOU AND STAY SAFE.

© 2023, Motorola Solutions. All rights reserved. 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.

State of New Jersey
OFFICE OF THE ATTORNEY GENERAL
DEPARTMENT OF LAW AND PUBLIC SAFETY
DIVISION OF CRIMINAL JUSTICE
PO BOX 085
TRENTON, NJ 08625-0085
TELEPHONE: (609) 984-6500

PHILIP D. MURPHY
Governor

SHEILA Y. OLIVER
Lt. Governor

MATTHEW J. PLATKIN
Attorney General

PEARL MINATO
Director

ATTORNEY GENERAL LAW ENFORCEMENT DIRECTIVE NO. 2022-12

TO: All Law Enforcement Chief Executives and County Prosecutors

FROM: Matthew J. Platkin, Attorney General

DATE: October 21, 2022

SUBJECT: Updated Directive Regulating Use of Automated License Plate Recognition (ALPR) Technology

In 2010, Attorney General Law Enforcement Directive 2010-5 established statewide guidelines governing the use of automated license plate recognition (ALPR) technology and the data it generates.[1] After more than a decade of experience with what was then an emerging technology, an updated policy on ALPRs is necessary.

This update has two major goals. First, it maintains—and builds upon—the significant safeguards from abuse and privacy protections that have served the State well under the 2010 policy, including continuing to apply the New Jersey Supreme Court's framework in State v. Donis, 157 N.J. 44 (1998), limiting law enforcement access to personal identifying information associated with a vehicle's license plate unless there is a particularized basis. Second, the revised policy facilitates the sharing and standardization of ALPR data statewide in order to maximize our ability to use this tool to solve and prevent crimes.

The major revisions are as follows. Additionally, other portions of the 2010 policy have been reorganized or condensed.

- ***Oversight***. Establishes ALPR coordinators at the agency, county, and state level to improve oversight and information sharing.

- ***Sharing and standardization of data***. Requires use of the statewide application program

[1] "Automated license plate recognition" or ALPR is technology that uses optical character recognition on images to read vehicle registration plates to create vehicle location data. ALPR devices may be placed at a stationary location (permanent or portable) or be mobile and affixed to a police vehicle. The vehicle location data captured by an ALPR device is (1) used to alert law enforcement to vehicles they have a legitimate and specific reason to locate, and (2) stored so that law enforcement may perform searches to further subsequent investigations. Both situations are described in more detail in this Directive.

interface ("Statewide API")—software that will make ALPR data accessible statewide—and mandates standard data formats to make ALPR information consistent across agencies, without requiring additional agreements between agencies.

- ***Retention period***. Decreases retention period for both ALPR data and records from five years to three years.

- ***Release of ALPR data***. Lays out release process for ALPR data in criminal prosecutions.

- ***Audits***. Mandates annual audits of each agency's ALPR program.

- ***Training***. Establishes specific training requirements for all agency users authorized by their law enforcement executive to use ALPRs and access ALPR data.

Therefore, pursuant to the authority granted to me under the New Jersey Constitution and the Criminal Justice Act of 1970, N.J.S.A. 52:17B-97 to -117, which provides for the general supervision of criminal justice by the Attorney General as chief law enforcement officer of the State in order to secure the benefits of a uniform and efficient enforcement of the criminal law and the administration of criminal justice throughout the State, I hereby direct all law enforcement and prosecuting agencies operating under the authority of the laws of the State of New Jersey to implement and comply with the directives outlined below.

1. **Oversight**

1.1 ***Agency***. The law enforcement executive of each agency using an ALPR or its data shall designate an Agency ALPR Coordinator who will:

- Be the external point of contact for agency ALPR-related items such as information sharing and audits;

- Internally oversee the agency's ALPR program, including training and approving access requests (may delegate approval authority to other supervisors);

- Designate authorized users within the agency who can use ALPRs and access stored data (such users must complete the trainings mandated by this Directive).

1.2 ***County***. Each County Prosecutor will designate a County ALPR Coordinator who will maintain contact information for Agency ALPR Coordinators in the county and provide it to the State ALPR Coordinator. Where county ALPR data is maintained by a sheriff's department or public safety agency, a representative from that agency may be designated as a County ALPR Co-Coordinator. State agencies should report their Agency ALPR Coordinators directly to the State ALPR Coordinator.

1.3 ***State***. The Attorney General, in consultation with the New Jersey State Police ROIC Commander, will designate a State ALPR Coordinator to oversee the "Statewide API" that connects stored ALPR data (discussed below) and the state's ALPR program generally.

2. Deployment

2.1 ***Official use only***. An ALPR and the data it generates shall only be used for official and legitimate law enforcement purposes. The agency's law enforcement executive or designee must authorize deployment of each ALPR.

2.2 ***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, 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).

2.3 ***Sharing deployment information***. The following data must be shared with the State ALPR Coordinator prior to installing or relocating a permanent fixed ALPR unit:

- Camera name (pursuant to convention specified by State ALPR Coordinator)
- Location (latitude and longitude)
- Survey provided by ALPR vendor, including projected size of ALPR data

When deploying or relocating a portable fixed ALPR unit, agencies must provide updated latitude and longitude data to the State ALPR Coordinator.

2.4 ***Deconfliction***. Agency ALPR Coordinators shall deconflict with the County and State ALPR Coordinator about deployment locations to avoid duplication of efforts.

3. BOLO lists

3.1 ***Standard for including license plate in BOLO list***. A license plate number may be included in a "be on the lookout" or BOLO list (a compilation of license plates or partial plates for which a BOLO situation exists) for input into an ALPR system only if there is a legitimate and specific law enforcement reason to identify or locate that particular vehicle, or any person(s) 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/SILVER alerts
- Vehicles and/or persons involved in prior suspicious activity, such as groups of vehicles travelling together suspected of criminal activity, or subjects trying to open doors to random cars
- Stolen vehicles
- Vehicles reasonably believed to be involved in the commission of a crime or disorderly persons offense
- Vehicles registered to or 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
- Persons who are on any watch list issued by a state or federal agency responsible for homeland security

3.2 ***Batch downloading***. 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, US Department of Homeland Security, and Motor Vehicle Commission database.

3.3 ***Updating BOLO lists***. A BOLO list may be revised at any time. Updates to a BOLO list shall be done at the start of each shift for mobile ALPRs attached to police vehicles, and as frequently as possible, but at least daily, for ALPRs at stationary locations.

3.3.1 All ALPR systems must provide an Application Program Interface (API) or web service to update in real-time a BOLO list(s) through methods approved by the State ALPR Coordinator, including AMBER/SILVER alerts that remain on the list until expired or withdrawn.

3.4 ***Immediate alert response***. A BOLO match with an ALPR scan may be programmed to trigger an immediate alert. The reason for including the vehicle on the BOLO list shall be disclosed to the officer who will react to an immediate alert. The officer should determine whether the alert has been designated as a non-encounter alert (meaning officer should not encounter the vehicle) and, if so, follow any instructions included in the alert for notifying the originating agency.

3.4.1 When an officer receives an immediate alert without a non-encounter restriction, the officer shall take such action in response to the alert as is appropriate in the circumstances. An officer alerted 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 NJ. Super. 407 (App. Div. 1996) (no reasonable suspicion to justify a stop because registered car owner's license suspended unless driver generally matches the owner's physical description (e.g., age and gender)).

4. Accessing stored data

4.1 ***Alert data***. An authorized user may access and use stored ALPR alert data (i.e., ALPR license plate data matching an entry on a BOLO list) as part of an active investigation or for any other legitimate law enforcement purpose, including but not limited to a BOLO query, a crime scene query, or crime trend analysis (as defined below).

4.2 ***Non-alert data***. Access to and use of stored non-alert ALPR data (i.e., ALPR data gathered not matching a BOLO list entry) is limited to the following three purposes explained below: a BOLO query, a crime-scene query, and crime trend analysis (system tests and troubleshooting are also acceptable purposes).

4.2.1 BOLO query. Agencies may compare a BOLO list against stored non-alert 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 subsequently be placed on an active BOLO list (for example, may review data to determine whether a specific vehicle was present at the time and place where the ALPR data was initially scanned to check an alibi defense or to develop lead information for the purpose of locating a specified vehicle or person; or to determine whether a vehicle that was only recently added to a BOLO list had been previously observed in the jurisdiction before being placed on the list).

4.2.2 Crime scene query. Agencies may 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 (i.e., incident that would constitute an indictable crime under New Jersey law). Such queries may not be conducted to review data based on general crime patterns (e.g., to identify persons traveling in or around a "high crime area"). A record shall be kept of the specific crime(s) justifying the query, including the crime date and location.[2]

4.2.3 Crime trend analysis. Agencies may access and use stored non-alert data where such access, which may be automated, might reasonably lead to the discovery of evidence or information relevant to an investigation that is not related to a specific criminal event. Such access must be approved by the Agency ALPR Coordinator or their designee.

Crime trend analysis shall not result in the disclosure of personal identifying information (such as name, address, SSN, vehicle operator's license number) to an authorized user or any other person unless (a) there exist "specific and articulable facts that warrant further investigation" of possible criminal or terrorist activity by the driver or occupants of a specific vehicle and access has been approved by a designated supervisor; or (b) disclosure of personal identifying information concerning any vehicle plate scanned by the ALPR is authorized by a grand jury subpoena.[3]

[2] A crime scene query shall be limited in scope to 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 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). In contrast, a spontaneous crime might reasonably justify examining data that was scanned and collected on or about the time of and in closer physical proximity to the criminal event.

[3] 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

Any crime trend analysis shall document:

- The nature and purpose of the crime trend analysis
- The authorized users who accessed stored non-alert data
- The designated supervisor who approved access
- Where personal identifying information was disclosed, (a) the specific and articulable facts that warrant further investigation and (b) the designated supervisor who approved the disclosure of personal identifying information; or, where applicable, the fact that a grand jury subpoena authorized access to personal identifying information.

4.3 ***Documenting access for any stored data search***. A record shall be made of the authorized user accessing stored ALPR data and the date, and for non-alert data the record should include the justification for access. Once stored data has been accessed and transferred to an investigation file by an authorized user, it shall not be necessary after that to document further access or use of that data pursuant to this Directive.

5. Sharing data

5.1 ***Statewide API***. The State ALPR Coordinator shall implement a "Statewide API" (application program interface) that allows access to stored ALPR data across agencies, and specify the method by which all ALPRs used by New Jersey agencies must provide real-time access to ALPR data through the API. Agencies may also share data regionally with other New Jersey agencies pursuant to the mandates of this Directive, and ALPR data collected by a private entity that has entered into an agreement with New Jersey law enforcement can be shared with New Jersey agencies. All ALPRs must make data available to the Statewide API by the effective date of this Directive, and subsequent ALPRs must do so within 45 days of deployment. ALPR systems must be programmed to capture data parameters and meet minimum requirements for accuracy and performance as specified by the State ALPR Coordinator.

5.2 ***Sharing with agencies not covered by this Directive***. An agency may enter into a written agreement to share ALPR data with, or receive data from, a law enforcement agency outside of New Jersey or otherwise not covered by this Directive with the approval of the State ALPR Coordinator. Only federally recognized law enforcement agencies may receive access to a New Jersey agency's ALPR data. The State ALPR Coordinator may agree to share ALPR data with a law enforcement agency outside of New Jersey if the out of state agency agrees in writing to use the data only for documented, legitimate law enforcement purposes and to follow other restrictions required by the State ALPR Coordinator in order to achieve 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).

objectives of this Directive. Private entities may provide ALPR data to New Jersey agencies but cannot receive law enforcement-owned ALPR data.

6. Storage, records, and retention

6.1 ***Storage of ALPR data***. All ALPR data shall be stored securely and maintained electronically with access restricted to authorized users. ALPR data shall be the property of the agency and not any ALPR vendor. Agencies may jointly store their ALPR data. Commercially obtained ALPR data shall not be co-mingled with law enforcement data. Data being used in an investigatory process shall be maintained in accordance with the agency's evidence or records management procedures.

6.2 ***Deployment records***. Agencies shall maintain the following information regarding each ALPR owned or operated:

- Date and time deployed
- Portable or fixed
- Identity of operator
- Vendor name
- Date ALPR data connected to Statewide API (for agencies that house ALPR data)

6.3 ***Stored ALPR data access records***. Agencies that store ALPR data shall maintain an automated record-keeping of all access to stored ALPR data (in the case of county storage, the county may keep access records instead), including the following:

- Date and time of access, and for non-alert data, the justification for access
- Authorized accessor name
- Whether an automated software program was used to analyze the data
- Designated supervisor who approved disclosure of personal identifying information based upon crime trend analysis
- Instances of testing or troubleshooting an ALPR system
- Any other information required to be documented under this Directive

6.4 ***Retention***. Records and ALPR data covered by this Section shall be retained for three years.

6.4.1 ALPR stored data shall be purged after the retention period, unless it is associated with an active investigation or pending judicial process, in which case the data should be exported from the relevant storage system and retained in the case file.

6.4.2 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 required retention and purging period.

6.4.3 Records shall be kept in a manner that makes them readily accessible for audit.

7. Discovery

7.1 ***Criminal investigatory records***. 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 a subpoena or court order authorizes such disclosure or unless such disclosure is required by court rules governing discovery in criminal matters.

7.1.1 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 Director of the Division of Criminal Justice (DCJ)).

7.2 ***Release of ALPR data***. If ALPR data is accessed as part of an investigation—including but not limited to a BOLO query, a crime scene query, or crime trend analysis—a record of the access, which may be automated, and corresponding data shall be included in the agency's investigative file (electronic or physical). If the investigation results in criminal charges, the ALPR records shall be turned over in discovery pursuant to applicable court rules and case law.

8. Compliance

8.1 ***Establishing a policy***. Agencies that possess or use an ALPR or its data shall establish—or conform existing—standing operating procedures, directives, or orders that govern ALPRs and stored ALPR data consistent with this Directive before the Directive takes effect (ninety days after issuance). The law enforcement executive shall provide a copy of the agency's ALPR policy to the County Prosecutor (or DCJ Director) and County and State ALPR Coordinator at or before the time of promulgation, including any subsequent policy amendments.

8.2 ***Violations***. Any knowing violation of this Directive or related agency standing operating procedure, directive, or order, or applicable law, shall be subject to discipline.

8.2.1 All significant violations of this Directive or agency policy, including but not limited to unauthorized access or use of ALPR stored data, must be reported to the County Prosecutor (or DCJ Director) and County and State ALPR Coordinator upon discovery. 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 law enforcement executive and with notification to the State ALPR Coordinator, 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.

8.2.2 Any complaints about an agency's ALPR program made by any citizen or entity shall be forwarded to the appropriate County Prosecutor (or DCJ Director), for appropriate review and handling, as well as notification to the County and State ALPR Coordinator. The County Prosecutor or Director may conduct an investigation or direct the agency that is the subject of the complaint to conduct an investigation and

report back to the County Prosecutor or Director, with notification to the State ALPR Coordinator.

8.2.3 If the Attorney General or their designee has reason to believe that a law enforcement agency is not complying with or adequately enforcing the provisions of this Directive, 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 designee may initiate disciplinary proceedings and may take such other actions as the Attorney General, in their sole discretion, deems appropriate to ensure compliance with this Directive.

8.3 ***Audits***. By January 31 each year, the Agency ALPR Coordinator shall perform an audit of their agency's ALPR program and provide it to the County and State ALPR Coordinator.[4] That audit shall certify the following:

- Agency has an ALPR policy in place
- Only authorized users have accessed ALPR data
- Date of each authorized user's last ALPR training
- That a random survey of ALPR accesses revealed no misuse
- A description of any known significant violations and citizen complaints and whether they have been forwarded to the County Prosecutor or DCJ Director

The County ALPR Coordinator or State ALPR Coordinator may conduct an audit of an agency's ALPR program at any time.

8.4 ***Public reporting***. By March 31 each year, the State ALPR Coordinator shall publicly report the list of agencies that have completed audits, and the number of significant violations and citizen complaints reported by each agency.

8.5 ***Training***. The State ALPR Coordinator shall design and disseminate training on ALPR technology—including the application of this Directive and privacy and security considerations generally—that shall be a prerequisite for an individual being designated an authorized user under this Directive. Authorized users must complete refresher trainings every two years, as determined by the State ALPR Coordinator.

9. <u>Other provisions</u>

9.1 ***Attorney General exemptions***. ALPRs, and all ALPR stored data, shall only be used and accessed as authorized by this Directive. However, the Attorney General or their designee may authorize the specific use of an ALPR or the data it generates that is not expressly authorized by this Directive. Any request by a department to use an ALPR or ALPR-generated data for a purpose or in a manner not authorized by this Directive shall be made to the Attorney General or their designee through the DCJ Director. Such requests shall be made

[4] Where appropriate, a County Prosecutor may perform an agency's audit in place of the Agency ALPR Coordinator. The State ALPR Coordinator will audit the New Jersey State Police ALPR program.

in writing unless the circumstances are exigent, in which case approval or denial may be given orally and memorialized in writing as soon thereafter as is practicable.

9.2 ***Non-enforceability by third parties***. This Directive is issued pursuant to the Attorney General's authority to ensure the uniform and efficient enforcement of the laws and administration of criminal justice throughout the State. This Directive imposes limitations on law enforcement agencies and officials that may be more restrictive than the limitations imposed under the United States and New Jersey Constitutions, and federal and state statutes and regulations. Nothing in this Directive shall be construed in any way to create any substantive right that may be enforced by any third party.

9.3 ***Severability***. The provisions of this Directive shall be severable. If any phrase, clause, sentence or provision of this Directive is declared by a court of competent jurisdiction to be invalid, the validity of the remainder of the document shall not be affected.

9.4 ***Questions***. Any questions concerning the interpretation or implementation of this Directive shall be addressed to the DCJ Director or their designee.

9.5 ***Effective date***. This Directive shall take effect on January 23, 2023, which is approximately ninety days after issuance. The provisions of this Directive shall remain in force and effect unless and until it is repealed, amended, or superseded by Order of the Attorney General.

9.6 ***Prior directives***. This Directive supersedes any prior directive on this topic, including Law Enforcement Directive 2010-5 and its November 18, 2015 revision.



Matthew J. Platkin
Attorney General

ATTEST:



Lyndsay V. Ruotolo
First Assistant Attorney General

Dated: October 21, 2022

COMFORT SYSTEMS USA
BCM Controls Corporation

ALWAYS ON
CUSTOMER CARE PROGRAM

Service Agreement Proposal

Mass State Police - AirLink Device Management Service Renewal (2023)

Quote # Q006549-BCM
Version 1

Prepared for:

Massachusetts State Police

Noah Pack
noah.pack@state.ma.us

30 Commerce Way
Woburn, MA 01801
www.bcmcontrols.com
781-933-8878

1549

COMFORT SYSTEMS USA
BCM Controls Corporation

Tuesday, June 27, 2023

Massachusetts State Police
Noah Pack
470 Worcester Road
Framingham, MA 01702
noah.pack@state.ma.us

Dear Noah,

Thank you for providing BCM Controls with the opportunity to support you and your Security Systems. BCM's industry-leading services are designed to keep your system in top operating condition as well as to provide a level of engagement aimed at helping to prepare you for the needs of today and those into the future. Our service program consists of various features and benefits, as illustrated in this proposal.

Pricing assumes that the agreement will be in place before 07/01/2023 and that the agreement will remain in place from 07/01/2023 through 09/30/2024.

We value your business.

Sincerely,

Matt Boschetto
Account Manager
BCM Controls-MA

30 Commerce Way
Woburn, MA 01801
www.bcmcontrols.com
781-933-8878

COMFORT SYSTEMS USA
BCM Controls Corporation

Sustainment Services

Product Details

Subscription Services



Subscription Services are another emerging service area that will enable BCM's clients to subscribe to software-based offerings in lieu of purchasing them outright.

Subscription Services will be predicated on monthly, quarterly, semi-annual or annual billing, allowing clients to opt-out of individual services when they are no longer needed or relevant.

Included

Per your request, the following Subscription Service plans will align with a September 30th 2024 expiration. These services will need to be renewed annually at the aligned expiration date.

Sierra Wireless - AirLink Basic Remote Device Management

The proposed Subscription Services Plan provides services listed below:

Detailed Description:

10 - *AirLink Basic Remote Device Management (July 1, 2023 to Sept 30, 2024)*

123 - *AirLink Basic Remote Device Management (Oct 1, 2023 to Sept 30, 2024)*

1 - *AirLink Basic Remote Device Management (Nov 1, 2023 to Sept 30, 2024)*

5 - *AirLink Basic Remote Device Management (May 1, 2024 to Sept 30, 2024)*

30 Commerce Way
1551
Woburn, MA 01801
www.bcmcontrols.com
781-933-8878

COMFORT SYSTEMS USA
BCM Controls Corporation

Clarifications

- Content in this proposal is intended to provide a summary description for the services offered pending execution of Always On Service Level Agreement contract documents.
- Remote access to customer's security platforms will require customer-provided and maintained VPN access

Privileged Information Statement

The information contained in this document and the solution proposed by BCM Controls Corporation (BCM) is proprietary and confidential to BCM. These materials can be used solely for the purpose of evaluating a possible transaction between BCM and its prospective customer. No recipient of these materials may use them for their own commercial advantage. The recipient of these materials must hold them in confidence and shall not distribute them, in whole or in part, to any other individual or entity in any form without the prior written consent of BCM.

30 Commerce Way
Woburn, MA 01801
www.bcmcontrols.com
781-933-8878

COMFORT SYSTEMS USA
BCM Controls Corporation

Mass State Police - AirLink Device Management Service Renewal (2023)

Prepared by:

BCM Controls-MA
30 Commerce Way
Woburn, MA 01801
Matt Boschetto
781-528-8344
boschettom@bcmcontrols.com

Prepared for:

Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Noah Pack

noah.pack@state.ma.us

Quote Information:

Quote #: Q006549-BCM
Version: 1
Delivery Date: 06/27/2023
Expiration Date: 08/25/2023

Quote Summary

Description	Amount
Pricing Summary	$4,816.23

Total: **$4,816.23**

Payment Options

Description	Payments	Interval	Amount
Service Agreement			
One Year Term / Paid in Advance	**1**	**One-Time**	**$4,816.23**

Taxes, shipping, handling and other fees may apply. We reserve the right to cancel orders arising from pricing or other errors.

BCM Controls-MA

Signature: _____
Name: Matt Boschetto
Title: Account Manager
Date: 06/27/2023

Massachusetts State Police

Signature: _____
Name: Noah Pack
Title: Sergeant
Date: _____

30 Commerce Way
Woburn, MA 01801
www.bcmcontrols.com
781-933-8878

COMFORT SYSTEMS USA
BCM Controls Corporation

AO MA ITC71 - Terms & Conditions

ITC-71

All provisions of the Service Agreement are governed and in compliance with the Commonwealth of Massachusetts procurement contract ITC71.

Exclusions

The following are excluded from this Agreement. Any materials or services provided by BCM Controls due to the following will be invoiced separately on a Time and Material basis with payment due Net 30 days.

- Improper Operation - Repairs due to improper or incorrect operation procedures by the Customer or others, negligent maintenance by the Customer or others, misuse or excessive wear and tear of System equipment and relocation of System equipment by Customer or others.
- Modifications. This Agreement covers the System as installed under the manufacturer's guidelines and specifications for the intended use of the product. Modifications to the System to rectify improper installations by vendors other than BCM Controls are not included under the Agreement.
- Consumable Goods. Tags, Cards, r bbons, paper, supplies and other consumable goods.
- Governmental Requirements. System design changes required in order to comply with governmental authorities, Fire Marshal, etc.
- Existing Defects. Any deficiencies in or damages to the System caused solely by Massachusetts State Police found during the first complete inspection by BCM Controls . BCM Controls will offer a quotation to repair or replace such items.
- Obsolete and Unrepairable Materials. Materials no longer manufactured or repairable at a reasonable cost will not be maintained. Non-repairable items will be quoted to be replaced.
- Bucket Trucks and/or lifts, if required, are the owners responsibility unless specified in the agreement. If BCM is to provide, the costs will be billed to the customer.
- Other Exclusions. Software; repairs or replacements due to vandalism, flooding, fire, lightning, power failure or surges, brownouts, acts of God or similar phenomenon, or any other cause beyond the control of BCM Control.

Work Hours / Time and Material Rates

This agreement is inclusive of labor as applicable by the terms and conditions set forth. Non-covered services during "Normal Business Hours" and/or "Non-Business Hours", as applicable, will be billed at labor rates listed below.

Work Hours are defined as follows:
Normal Business Hours: 8:00AM - 5:00PM Monday - Friday, Excluding Holidays
Non- Business Hours: 5:00PM - 8:00AM Monday - Friday, Weekends and Holidays

Labor Rate Schedule for work that is not included in this agreement are as follows**:

$148/hr: Technician - Hourly during Business Hours
$211/hr: Technician - Hourly during Non-Business Hours
$179/hr: Remote Services - Hourly during Business Hours
$255/hr: Remote Services - Hourly during Non-Business Hours
$184/hr: Engineering / Programming - Hourly during Business Hours
$259/hr: Engineering / Programming - Hourly during Non-Business Hours

**Labor Rate Schedule is as per ITC71.

Communications Equipment and Services

Customer acknowledges that signals are transmitted over an internet connection, regular phone lines or network service, and that such telephone or network service is the sole responsibility of the customer, and that in the event internet connection, telephone or network services is out of order, disconnected, or otherwise interrupted, circumvented or compromised, signals will not be received by the system during the interruption and the interruption will not be known to BCM Controls. You will immediately report (i) problems with the communications equipment or communications services to the communications provider; and (ii) problems with the System to BCM Controls for repair service. You will pay all charges for communications equipment and communications services, including any charges for the installation, modification or repair of such communications equipment and communications services.

Increase in Charges

Any equipment additions may result in additional costs to the service agreement. BCM Controls will add the charges for the additional equipment on the anniversary of the contract. All service costs from completion of the installation until the anniversary will be included in the project costs.

30 Commerce Way
Woburn, MA 01801
www.bcmcontrols.com
781-933-8878

COMFORT SYSTEMS USA
BCM Controls Corporation

AO MA ITC71 - Terms & Conditions

Default

If you default under this Agreement, BCM Controls will provide written notice. If default is not cured within thirty (30) business days of notice, BCM Controls shall be entitled to retain all prepayments received and you shall immediately pay BCM Controls all payments then due and payable through the end of the service year and, BCM Controls shall have no further obligation to perform under this Agreement, upon your default. BCM Controls purchases software support agreements and warranties on an annual basis, requiring the customer to complete the year.

Binding Agreement

This Agreement only becomes binding upon BCM Controls when signed by BCM Controls' authorized representative or upon the commencement of any of the Services. This Agreement is binding on the parties' heirs, executors, administrators, successors and permitted assigns.

Assignment

This agreement and its benefits are not assignable by either party except upon the prior written consent of the other party. Customer acknowledges that this Agreement and particularly those paragraphs relating to BCM Controls' maximum liability and indemnification, inure to the benefit of, and are applicable to any assignees or subcontractors of BCM Controls and/or its affiliates.

Delays in Service

You acknowledge that there may be interruptions of service or delays in performing the services. BCM Controls' sole obligation after receiving a service request from you will be assigned to a team member within a reasonable time period once the team member becomes available, during normal business hours excluding Saturdays, Sundays and holidays.

Remote Services

The remote services group is your greatest asset. BCM Controls built the group to deliver speed of service, continuity and not to roll vehicles, all saving costs. To that end, BCM Controls will need remote access to the onsite equipment. BCM Controls may add software to existing servers or those provided during the install. If the customer does not allow access the costs of service may escalate. Customer's IT staff will be an integral part of the solution and will be required to maintain connectivity for the BCM Controls remote team.

Limited Warranty

BCM Controls warrants to you alone only that equipment we are obligated to install, is installed in a good and workmanlike manner. If any part, becomes defective within 90 days of the installation, BCM Controls shall repair or replace the defective part without charge to you. If you select the warranty period specified, BCM Controls shall repair or replace the defective part without charge to you, for the term of the agreement. System defects must be identified in writing and emailed to the service department at BCM Controls so that immediate corrective action may be taken. This warranty does not cover damage to equipment to equipment caused by accident, vandalism, customer negligence, flood, water, lightning, fire intrusion, abuse, misuse, terrorism, acts of God, any casualty including electrical charges, attempted unauthorized repair service, modification or improper installation by anyone other than BCM Controls, or any causes other than wear and tear.

Valid Agreement

Should any provision hereof (or portion thereof), or its application to any circumstances, be held illegal, invalid or unenforceable to any extent, the validity and enforceability of the remainder of the provision and this Agreement, or of such provisions as applied to any other circumstances, shall not be affected thereby, and shall remain in full force and effect as valid, binding and continuing.

Modifications

All changes or amendments to this Agreement must be in writing and signed by all parties to be binding on the parties.

Additional Equipment or Service

If, at any time after the date hereof, you request or authorize additional equipment or services, all sales, installation and services supplied by BCM Controls shall be subject to the terms of this Agreement only, except that additional charges shall be made for such additional sales, installation or services.

Functional Obsolescence

Materials no longer manufactured or repairable at a reasonable cost will not be maintained. Non-repairable items will be replaced and invoiced additionally with the customer's approval.

30 Commerce Way
Woburn, MA 01801
www.bcmcontrols.com
781-933-8878

COMFORT SYSTEMS USA
BCM Controls Corporation

AO MA ITC71 - Terms & Conditions

Right to Notice and Cure

Either party may terminate this agreement at any time for breach of any material term or condition by the other party, provided however, non-breaching party must provide the other party with five (5) business days written notice of the existence of an allegation with a detailed description of such breach. In the event such breach is not cured to the reasonable satisfaction of the non-breaching party, the non-breaching party shall have the right to terminate this Agreement at the end of that cure period with a written notice to the breaching party specifying the effective date of termination.

Right to Terminate

Notwithstanding anything set forth in this Agreement to the contrary, either party may terminate this Agreement, without cause and without any liability whatsoever, upon sixty (60) days' written notice.

Jurisdiction and Arbitration

Both parties to this agreement will be governed by the laws of the Commonwealth of Massachusetts and heard in the Massachusetts court system. Further both parties agreed to seek arbitration in the event of disagreement and will follow the American Arbitration guidelines. Each party will be respons ble for their own legal fees.

Electronic Media

A copy of this Agreement and signatures transmitted and delivered by facsimile or e-mail shall be deemed to be originals for all purposes. We may scan or otherwise convert this Agreement into an electronic and/or digital media file and a copy of this Agreement or the electronic Data file produced from any such electronic or digital media format may serve and be given the same legal force and effect as the original.

Insurance

BCM Control shall, at its own expense, for the duration of this Agreement and for two (2) years after the end of the Agreement, maintain policies of commercial general liability insurance including but not limited to product liability insurance and where appropriate professional liability insurance in an amount of at least One Million and 00/100 Dollars ($1,000,000.00) per occurrence and Three Million and 00/100 Dollars ($3,000,000.00) annual aggregate respectively to insure it, its employees, and its agents against all claims and liabilities arising out of or related to this Agreement. BCM Control liability aggregates can be satisfied by umbrella or excess liability policies.

Exclusion

Neither BCM Controls nor any BCM Controls subcontractor that provides Services under this Agreement has been excluded, suspended, debarred, or otherwise sanctioned from participation in any federal or state healthcare program, or has been convicted or found to have violated any federal or state fraud and abuse or illegal remuneration law. In the event that during the term of this Agreement, BCM Control or any of its agents are so excluded, suspended, debarred, or sanctioned or are convicted or found to have violated any federal or state fraud and abuse or illegal remuneration law, BCM Control shall promptly notify Customer of such event.

Indemnification

BCM Controls agrees to indemnify and hold armless Customer and Customer's directors, officers, agents and employees from and against all liabilities, losses , claims, suits, damages, cause of action, judgements or settlements of any kind or nature (including reasonable attorney's fees) asserted against Customer as a result of, arising out of, or relating to the acts or omissions of BCM Controls or its Directors, officers, employees, agents, contractors, or subcontractors committed directly or indirectly in the performance of this Agreement including, without limitation, any penalties and costs associated with fraudulent or illegal activities by BCM Controls. Customer agrees to indemnify and hold harmless the BCM Controls and BCM Controls' directors, officers, agents and employees from and against all liabilities, losses, claims, suits, damages, causes of action, judgments or settlements of any kind or nature (including reasonable attorney's fees) asserted against BCM Controls as a result of, arising out of, or relating to the acts or omission of Customer or its Directors, officers, employees, agents, contractors or subcontractors committed directly or indirectly in the performance of this Agreement including, without limitation, any penalties and costs associated with fraudulent or illegal activities by Customer.

Document Index				
Document Name	**Folder**	**Revision Date**	**Description**	**Effective Date**
ADM-01 Oath of Office	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/12/2023	All sworn members of the Department of State Police shall take and affirm an Oath of Office prior to the initial performance of duties.	6/25/2008
ADM-02 State Police Mission and Policy	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/12/2023	The Department of State Police, in cooperation with the Executive, Legislative, and Judicial branches of government, shall ensure that justice in a free society is perpetually prevalent.	6/25/2008
ADM-04 State Police Authority	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/12/2023	Within the Commonwealth, sworn members shall exercise all the powers of police officers as authorized by law and exercise professional discretion when appropriate.	6/25/2008
ADM-05 Organizational Structure	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/12/2023	The Department's organizational structure is arranged in a manner that simplifies the direction, coordination, and control of personnel.	1/29/2021
ADM-06 Command Staff Responsibilities	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/12/2023	The Command Staff is responsible for the administrative and operational control of the Department. Each member of the Command Staff shall maximize their involvement in the operations of the Department to deliver the highest level of public safety services to the citizens of the Commonwealth.	6/25/2008

557 ADM-07 Written Directives, Schedules and Forms	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	10/28/2021	The Department shall provide administrative direction and operational guidance through an internal written directive process.	1/22/2021
ADM-08 Strategic Planning	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	To provide effective management and planning, the Department shall: * Establish, review and revise a Multi-Year Plan; *Establish goals and objectives for the Department and each Division; * Continuously review, revise and track the progress of established goals and objectives; * Make established goals and objectives available to all agency personnel; * Annually review and revise written directives; and * Maintain a grant application process.	1/22/2021
ADM-08A Grant Approval Process	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	Whenever Department employees seek to obtain services and/or funding through private, public, state or federal entities; or to acquire or transfer equipment from an outside entity, the following procedures within this policy shall be adhered to.	11/5/2008
ADM-09 Line Inspection	Policy & Procedure / Rules & Regulations / Policy & Procedure	7/8/2022	Line Inspections shall be conducted to improve the operational readiness of the Department by ensuring that all members adhere to all established rules, regulations, policies, procedures, orders, directives, and general laws. Members shall immediately correct	4/23/2009

	Documents		unsatisfactory behavior and conditions in order to avoid the consequences which erode the trust and confidence of the public.	
ADM-09A Staff Inspections	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	The Department shall continuously audit and inspect all resources, facilities, equipment, personnel, practices and policies, to update the Command Staff on the quality of Department services.	1/22/2021
ADM-10 Awards	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/12/2023	The Department shall make every effort to recognize the people whose actions assist the Department in carrying out its mission and who go beyond normal expectations or requirements.	4/10/2018
ADM-11 Sick Leave	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/3/2021	The Department recognizes the importance of Sick Leave for its sworn members and their families. The Department has a responsibility to monitor the use of Sick Leave to prevent abuses.	4/16/2009
ADM-11A Temporary Modified Duty	Policy & Procedure / Rules & Regulations / Policy & Procedure	11/3/2021	Temporary Modified Duty is designed to provide an alternative work assignment for members who are temporarily unable to meet some of the Department in-service standards. Members failing to meet in-service medical and physical fitness standards due to temporary injury, illness or incapacitation are eligible to undergo	3/31/2017

559	Documents		reexamination pursuant to M.G.L. c. 22C, §10. Requests for reexaminations shall be made in writing to the Colonel/Superintendent within the period prescribed by M.G.L. c. 22C, §10 or shall be waived.	
ADM-11B Injury Reporting and Leave	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/4/2021	The Department shall investigate and document each on-duty injury to a member. All duty related injury documentation shall be completed and forwarded to the proper authority in a timely manner. Every injury shall be investigated in accordance with this policy.	6/25/2008
ADM-11C Maternity Leave and Guidelines	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/12/2023	The maternity policy is designed to provide notification and employment guidelines in order to prevent workplace discrimination on the basis of pregnancy.	6/25/2008
ADM-11E Leaves of Absence	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023	The Department may grant sworn and civilian employees leaves of absence, with or without pay, as allowed by: • Federal and state law; • Commonwealth's Human Resources Division (HRD); • Collective Bargaining Agreements (CBA), Personnel Administration Rules (PAR), HRD Red Book; or • The Colonel/Superintendent.	11/5/2008
	Policy &		The Department recognizes that the death or serious injury of a member is	

560 ADM-12 Serious Injury_Death of a Member	Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	traumatic and shall provide assistance to the member's family, recognizing that the needs of the family generally take precedence over the wishes of the Department	4/23/2009
ADM-13 Notification of Medical Examiner and_or Next of Kin	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	The Department shall promptly and compassionately notify the nearest relative of victims who have sustained life threatening injuries, or passed away.	4/23/2009
ADM-14 Internal Department Investigations	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023	To protect the integrity of the Department and to ensure continued public support: *All Department employees shall adhere to the Department's Policy and Procedure regarding external complaints (including anonymous ones) against any employee, policy, procedure, or operation of the Department; *All complaints shall be documented and investigated according to complaint intake procedures; and *Complaints, when assigned, shall be investigated at the lowest appropriate organizational level, unless determined otherwise by the Division of Standards and Training Commander or designee.	1/22/2021
			The Office of Professional Integrity and Accountability investigates allegations	

1561 ADM-15 Internal Affairs Investigations	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	of serious misconduct by employees of the Department or as ordered by the Office of the Superintendent or the Division of Standards and Training. The Office of Professional Integrity and Accountability also conducts Staff Inspections as outlined in ADM-09A.	1/22/2021
ADM-16 Notifying Prosecuting Agencies Regarding Evidence	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	Prosecuting agencies shall be notified of any and all Departmental investigations, to include personnel and/or internal affairs investigations, that are associated with an open criminal prosecution or investigation. Department employees who generate records, percipient witness statements, and/or evidence that relate to a criminal prosecution shall and must notify the appropriate agency prosecuting the case. The assigned lead Departmental investigator in any criminal or administrative investigation is responsible for ensuring such notification is made.	5/4/2018
ADM-17 Employee Evaluation System	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/12/2023	The Department shall continuously maintain an Employee Evaluation System (EES) to establish and measure performance expectations for sworn members. The EES shall be conducted in accordance with the Department's EES Manual.	6/25/2008

562 ADM-18 Unlawful Harassment Sexual Harassment and Discrimination	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/4/2021	The Department shall promote and maintain a working environment free from unlawful harassment, sexual harassment and discrimination.	8/1/2017
ADM-19 Vehicle Management	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/12/2023	To establish a central management system for all vehicles owned or controlled by the Department in order to maintain a state of operational readiness.	1/22/2021
ADM-19A Vehicle Use and Maintenance	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/12/2023	Department vehicles shall be maintained in a safe, clean and serviceable condition for reasons of safety, operational readiness, and to enhance the Department's public image. For the purposes of this policy only, members shall include sworn and civilian employees of the Department. Members assigned vehicles belonging to other authorities or governmental agencies, shall adhere to the vehicle use and maintenance policies of those particular authorities/agencies.	1/22/2021
ADM-19B Automated Vehicle Locater (AVL) Technology	Policy & Procedure / Rules & Regulations / Policy & Procedure	5/16/2023	The purpose of this policy is to establish guidelines and procedures for the use of the Department's Automated Vehicle Locator (AVL) Technology. AVL is designed to increase officer accountability and safety by enhancing the ability to rapidly locate and deploy Department personnel and resources. AVL	5/2/2018

563	Documents		technology also improves coordination and resource management during tactical situations, assists in improving response times to radio calls and increases situational awareness for all employees.	
ADM-20 Weapons Management	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/4/2021	The Armorer shall provide oversight for the control and operational readiness of all Department weapons and ammunition, from acquisition to final disposition. Members shall continually inspect all weapons and ammunition issued to them or under their control, to ensure cleanliness and operational readiness.	8/1/2017
ADM-21 Communications	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	The Department shall maintain an effective and efficient communications system to aid in the performance of its public safety mission. The Department shall ensure continuous communication accessibility through a mission-critical, multi-channel radio system capable of two-way operation on joint public safety frequencies. Dispatchers, Desk Officers and Troop Duty Officers shall use available technologies, including radio and Automated Vehicle Locator (AVL) to identify members potentially available for service and to maintain communication with	1/22/2021

			members. The Department shall comply with all Federal Communications Commission (FCC) procedures and requirements.	
ADM-22 Court Attendance and Fees	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	Department employees shall comply with all court orders and summons. Employees shall be compensated for court attendance according to their applicable collective bargaining agreements.	4/23/2009
ADM-24 Department Radio Call Signs	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/12/2023	The Department shall promote officer safety and efficiency using a standardized Radio Call Sign procedure. Standardized Radio Call Signs, as referenced within this General Order, shall be used by all employees for all radio transmissions.	1/22/2021
ADM-25 Paid Details and Overtime	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	2/21/2023	The Department may allow personnel, on full duty status or alternative duty status (as specified in ADM-11C Maternity Leave and Guidelines), to work paid details. The Department recognizes the importance of maintaining safe and efficient traffic flow at roadway work sites and special events. The Department also recognizes that at major sporting, civic, special events, and other times, members may be required to provide crowd control and/or security.	6/14/2018
	Policy & Procedure /		To establish and define	

ADM-26 Military Service	Rules & Regulations / Policy & Procedure Documents	5/12/2023	military service protocols for Department of State Police personnel.	6/25/2020
ADM-27 Transfers	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	12/5/2022	In order to maintain and enhance the operational functions of the Department, transfers may be made to: • Ensure adequate staffing levels; • Provide efficient public safety services; and • Meet other goals and objectives of the Department.	5/21/2018
ADM-28 Department Motor Vehicles	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	State owned vehicles shall be operated for official use only and in accordance with Policy and Procedure ADM-19 Vehicle Management and ADM-19A Vehicle Use and Maintenance.	3/1/2016
ADM-29 Workplace Violence	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	The Department shall maintain zero tolerance for workplace violence and ensure the workplace environment remains free from any form of violence. This policy does not apply to situations where members are exposed to threats or violent acts from persons in their care or custody, or the public at large, as an unavoidable component of the lawful performance of their law enforcement duties.	4/23/2009
			The Department shall conduct an Annual Fixed Asset Inventory. The Department shall: • Record and report Governmental Generally Accepted Accounting Principles (GAAP) Fixed Assets	

566 ADM-30 Asset Management	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/12/2023	of $50,000 or more within the Massachusetts Management Accounting and Reporting System (MMARS) twice per year pursuant to State Comptroller policy; • Maintain an automated Asset Management System that reflects all NonGAAP Fixed Assets with a useful life of one (1) year or more and a cost between $1,000 -$49,999; and • Maintain inventories of other assets in accordance with State Comptroller policy and as determined by the Division of Administrative Services.	6/14/2018
ADM-34 Information Technology Resources	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/12/2023	The Department shall regulate the use of Information Technology Resources (ITR), including computers, printers and other peripherals, programs, data, local and wide area networks, and use of the internet. ITR communications including email messages are considered public records, copies of which may be requested by the public.	4/23/2009
	Policy &		The personal use of social media can have bearing on departmental personnel in their official capacity. As such, this policy provides information of a precautionary nature as well as prohibitions on the use of social media by Department of	

567 ADM-34A Social Media Networking	Procedure / Rules & Regulations / Policy & Procedure Documents	5/12/2023	State Police Employees. When using social media/networking, Department Employees (sworn and civilian) should be mindful that their speech becomes part of the worldwide electronic domain. Department Employees should also be mindful to treat Department of State Police business as confidential per Rules and Regulations Article 5.	6/17/2013
ADM-35 Body-Worn and Cruiser-Mounted Cameras	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/4/2021		3/2/2021
ADM-36 Diversity and Equal Opportunity	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/4/2021	The Department prohibits discrimination in employment on the basis of race, color, religious creed, national origin, ancestry, gender, sexual orientation, Vietnam Era Veteran status, age, and disability.	11/5/2008
ADM-41 Telephone Use	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	The use of Department telephones should be limited to conducting official business and their use is subject to audit and review by the Department. Telephone communication shall be conducted in a professional manner providing information and assistance to callers as appropriate. Department members, including sworn and civilian members, shall adhere to all Massachusetts General Laws and MSP policy	1/22/2021

568			while utilizing cellular phones.	
ADM-46 Sexual Activity in Public Places	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	The Commonwealth of Massachusetts has a legitimate enforcement interest in ensuring that sexual activity and/or genital exposures do not occur in public places, where the likelihood of being observed by a casual passerby is reasonably foreseeable. Disparate enforcement of applicable statutes against any particular group and/or disparate treatment of any group is unacceptable.	4/23/2009
ADM-47 Bias-Based Policing	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	Except in "suspect specific incidents", members are prohibited from considering the race, national origin, ethnicity, sexual orientation/identity, socio-economic status, religion, immigration status, and/or age, gender identity or expression, cultural group, or disability, of members of the public in deciding to detain a person or stop a motor vehicle and in deciding upon the scope or substance of any law enforcement action. Bias practices are unfair, ineffective, promote mistrust, and perpetuate negative and harmful stereotypes. The Department is committed to bias-free policing.	1/7/2020
ADM-49 Deaf or Hard of Hearing Individuals	Policy & Procedure / Rules & Regulations / Policy &	5/12/2023		12/1/2021

1569	Procedure Documents			
Appendix "A"	Policy & Procedure / Rules & Regulations / Rules & Regulations	11/5/2021		1/31/2001
Article 1 - Regulations for the Governance of the State Police	Policy & Procedure / Rules & Regulations / Rules & Regulations	11/5/2021		1/31/2008
Article 10 Regulations Establishing Recruit Minimum Entrance Requirements	Policy & Procedure / Rules & Regulations / Rules & Regulations	11/5/2021		9/3/2019
Article 2 - Organizational Values	Policy & Procedure / Rules & Regulations / Rules & Regulations	11/5/2021		3/15/2021
Article 3 - Regulations Establishing the Duties Of Members	Policy & Procedure / Rules & Regulations / Rules & Regulations	11/5/2021		1/22/2021
Article 4 - Title and Rank, Payroll, Promotions	Policy & Procedure / Rules & Regulations / Rules & Regulations	11/5/2021		1/31/2001
Article 5 - Rules of Conduct	Policy & Procedure / Rules & Regulations / Rules & Regulations	11/5/2021		1/22/2021
Article 6 - Regulations Establishing Disciplinary Procedures and Temporary Relief from Duty	Policy & Procedure / Rules & Regulations / Rules & Regulations	11/5/2021		2/5/2001

570 Article 7 - Regulations Establishing Enlistment, Discharge and Resignation	Policy & Procedure / Rules & Regulations / Rules & Regulations	11/5/2021		6/25/2008
Article 8 - Regulations Establishing the Board on Claims	Policy & Procedure / Rules & Regulations / Rules & Regulations	11/5/2021		1/31/2001
Article 9 - Regulations Establishing Examination Appeal	Policy & Procedure / Rules & Regulations / Rules & Regulations	11/5/2021		1/31/2001
DET-01 Warrant Management	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/4/2021	Department members shall utilize established warrant management systems in accordance with federal and state laws and regulations and the contents of this policy.	1/22/2021
DET-01A Warrants, Summons, or Subpoenas	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/4/2021	In furtherance of a legitimate law enforcement purpose, members shall serve warrants, summons, or subpoenas once they become aware of their existence, or as otherwise ordered.	1/22/2021
DET-02 Custodial Inventory	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/4/2021	*To protect members and detainees from harmful items or substances that may have been concealed by the subject; *To protect members from claims of lost, stolen, or damaged property; and *To establish and define the processing of detainees who come under the care and custody of the Department.	1/22/2021
			Safety is the paramount	

1571 DET-03 Detainee Transportation	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/4/2021	concern when transporting detainees. Members shall always keep in mind: *The safety and well-being of themselves and others; *The proper restraint of the detainee to prevent escape or injuries; and *The detainee's safety and rights.	1/22/2021
DET-04 Holding Facility and Design	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/4/2021	The Department shall maintain holding facilities that comply with applicable laws and regulations, in order to provide a safe environment for members and detainees.	1/22/2021
DET-05 Identification of Persons in Department Custody	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/4/2021	All persons in Department custody must be properly identified prior to release. Fingerprints offer the most reliable means of individual identification. The submission and retention of fingerprint records and other biometrics create a reliable criminal history record. Therefore, all persons arrested shall be fingerprinted and photographed. In addition, all persons charged with a felony shall have their palmprints recorded if recording equipment is available. Persons taken into department custody for non-criminal reasons may be fingerprinted and photographed or may be identified through other means.	1/22/2021
			The safety and well-being of members and	

1572 DET-06 Detainee Monitoring	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/5/2021	detainees is the Department's paramount concern and shall guide the application of this policy. Continuous supervision is essential for maintaining and ensuring the safety and welfare of both detainees in custody and the members responsible for monitoring them. To ensure the safety of all, necessary precautions shall be taken whenever a person is taken into custody.	1/22/2021
DET-07 Detainee Sexual Abuse and Sexual Harassment	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/5/2021	In accordance with the Prison Rape Elimination Act (PREA) of 2003, the Department shall: * Establish a zero tolerance policy toward all forms of sexual abuse and sexual harassment towards any detainee; *Ensure that all detainees have the right to be free from sexual abuse and sexual harassment; and *Establish a zero tolerance policy toward all forms of retaliation against anyone who reports sexual abuse and sexual harassment or who cooperates in a sexual abuse investigation. This policy shall be made available through the Department's website and upon request.	1/29/2021
			As the investigative agency for alleged sexual crimes committed on adults and juveniles held in a confinement setting by	

1573 DET-07A Detainee Sexual Abuse and Sexual Harassment Investigations, Review, and Data Collection	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/5/2021	either the Department of Correction or Department of Youth Services, the Department of State Police shall ensure full compliance with the standards found within federal laws and mandates regarding the Prison Rape Elimination Act (2003). This policy shall be made available through the Department's website and upon request.	1/22/2021
DET-08 Gender Identity and Expression	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/5/2021	The Department strives to ensure that everyone it serves is treated with dignity, respect, and professionalism. Department employees shall not engage in conduct that denigrates or shows hostility toward an individual because of their gender identity or gender expression.	2/4/2021
DET-09 Juvenile Operations	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	12/1/2021	The Department shall ensure protection of Constitutional rights and compliance with Federal and Massachusetts laws and regulations regarding the detention of juveniles. Steps should be taken to determine if juveniles in custody of the Department are alleged to have been harmed or to be in danger of harm. Members shall adhere to mandated reporting requirements pursuant to SOC-07C.	1/22/2021
	Policy &		The Massachusetts State Police shall comply with the	

DET-10 Protective Custody	Procedure / Rules & Regulations / Policy & Procedure Documents	11/5/2021	requirements of Massachusetts General Law Chapter 111B and Massachusetts General Law Chapter 111E when taking an incapacitated person into protective custody.	1/22/2021
GEN-01 Personal Appearance	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/12/2023	As the principal law enforcement agency within the Commonwealth of Massachusetts, members shall present an image of the highest standard, order, and professionalism to the public. Members shall correct any deficiencies in their personal appearance, uniform, or equipment as soon as practicable, unless otherwise specified in this Order.	9/3/2019
GEN-01A Tattoos and Body Modifications	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/12/2023	Pursuant to GEN-01 Personal Appearance, members shall present an image of the highest standard, order, and professionalism to the public. Members of the Department shall maintain their personal appearance to the highest standards possible and in conformance with GEN-01 Personal Appearance.	6/22/2020
GEN-02 Uniforms	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	Members of the Department shall maintain their personal appearance and uniforms to the highest standards possible.	1/25/2018
GEN-04 Military Courtesy	Policy & Procedure / Rules & Regulations	7/8/2022	The Department has been a paramilitary organization since its inception; the application of military	4/23/2009

1575	/ Policy & Procedure Documents		courtesies shall continue to maintain this tradition.	
GEN-04A Ceremonial Tributes	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	The protocols identified within this policy shall be adhered to during ceremonial tributes in honoring Department members or when attending tributes with other agencies.	6/17/2013
GEN-05 Communicable Diseases	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	The Department shall provide its employees with equipment and information on communicable diseases to prevent exposure to dangerous and life-threatening diseases.	11/5/2008
GEN-06 Drug Testing	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	In order to ensure public safety and promote public trust, it is the policy of the Department to maintain a drug-free work environment.	11/5/2008
GEN-07 Automatic External Defibrillators	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/5/2021	The Department maintains Automatic External Defibrillators (AED) to help save lives. Only Department members trained in the use of AED's may operate them.	4/23/2009
GEN-08 Ride Along_Observer	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/5/2021	The Department may allow approved ride-along/observers to accompany onduty members for educational purposes.	11/5/2008
INV-01 Criminal Investigations	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	Investigations shall be conducted on all matters of a criminal nature that fall within the jurisdiction of the Department.	1/22/2021
			Case management is an ongoing process	

1576 INV-01A Case Management	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	involving all members of the Department. Proper case management facilitates the scope and direction of an investigation, in addition to providing documentation for the Department and court proceedings.	1/22/2021
INV-02 Confidential Informants	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	The Department shall develop and use confidential informants, as well as other sources of information, as a means to detect, investigate, and prosecute violators of state and federal law.	6/14/2018
INV-02A Confidential Funds	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/5/2021	Confidential funds may be used to further investigations, and shall be carefully monitored and supervised.	4/23/2009
INV-03 Prescription Monitoring Program	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/12/2023	The purpose of the Prescription Monitoring Program is to assist health care providers and investigative agencies in addressing drug diversion and the misuse and abuse of pharmaceutical controlled substances.	5/21/2018
INV-05 Special Protections for Juveniles	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/5/2021	Courts recognize the vulnerability of children. The Department shall ensure that juveniles are afforded special protections during interrogations.	7/12/2018
INV-07 Non-Published Telephone Numbers	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/12/2023	Telephone company records shall only be obtained when necessary for the furtherance of a criminal investigation or in an emergency.	5/21/2018

1577 INV-08 Criminal Intelligence	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/2/2021	The Department shall share criminal intelligence among the criminal justice community in an effort to prevent and control crime, while protecting the privacy and constitutional rights of individuals.	5/21/2018
INV-09 Polygraph Examinations	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	he polygraph is a reliable investigative tool when used by a professional examiner. The Department shall use the polygraph with great selectivity, and then, only as an investigative tool.	1/22/2021
INV-10 Evidence Collection and Preservation	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	The Department shall ensure that evidence is properly recognized, documented, collected, packaged, and stored; and shall ensure that a chain of custody is established for evidence recovered at every crime scene.	1/22/2021
INV-11 Controlled Substance Intake-Storage	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	The Department shall establish rigid controls for all controlled substances held within its custody to preserve the integrity of the Department and its personnel. Through the assignment of responsibilities, processing procedures, storage requirements and continuous inspections, all levels of command shall ensure strict compliance with established controls and this policy.	5/10/2012
			The Department shall establish procedures for all evidentiary, found, seized, recovered, impounded, abandoned,	

INV-11A Evidence/Contraband/Property Intake-Storage	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	or unclaimed property including contraband held within its custody to preserve the integrity of the Department and its personnel. A written report shall document the circumstances by which said property came into the Department's possession and detail each item of property. All levels of supervision shall ensure compliance with established procedures within this policy regarding processing, storage requirements, and inspection.	1/22/2021
INV-13 Asset Forfeiture	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	The Department shall adhere to state and federal forfeiture laws involving illegal activities.	4/23/2009
INV-14 Seized Currency	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	The Department shall establish rigid controls and strict accountability for all seized currency coming into its custody. A non-interest bearing cashless system shall be utilized to ensure that all seized currency is properly accounted for, secured, stored, and readily retrievable. Any changes in the custody of any seized currency shall be appropriately documented.	1/29/2021
INV-15 Field Interview and Observation Reports	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/2/2021	Members shall follow the established guidelines for the collection, security, and dissemination of information gathered through field interviews and observations.	4/23/2009

579 INV-16 Electronic Recording of Interrogations	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	Members shall, whenever it is practical, electronically record all custodial interrogations of suspects or interrogations of suspects conducted in places of detention.	4/23/2009
INV-16A Eyewitness Identification	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	Eyewitness identification frequently plays an important role in Department investigations and it is absolutely critical that eyewitness evidence be accurate and reliable in order to ensure that the highest possible quality of evidence is obtained. The Department recognizes the importance of conducting and documenting eyewitness identification information in accordance with established guidelines, while recognizing that members are free to exercise discretion in adapting these guidelines to fit the unique circumstances of each case.	1/22/2021
INV-17 Travel-Immigration Status Inquiries and Investigations	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	Investigating and enforcing violations of federal immigration law is not a mission of the Massachusetts State Police. Accordingly, it is not appropriate for a member of the State Police to inquire about a non-citizen's immigration or travel status for the sole purpose of facilitating that person's detention or deportation by U.S. Immigration & Customs Enforcement	8/1/2017

580			(ICE).	
INV-18 Mobile Identification Device Use	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	This policy provides guidelines for the issuance, training, and use of Mobile Identification Devices. Authorized and trained Members may access the Department's Automated Fingerprint Identification System and the Next Generation Identification system by the State Identification Section (SIS) for the use of Mobile Identification Devices to assist in the identification of individuals under appropriate circumstances and to provide for additional officer safety and situational awareness.	1/22/2021
INV-19 Use of Facial Recognition Technology	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	12/1/2021		12/1/2021
INV-20 Covert Audio Recordings	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	6/29/2023		6/29/2023
Policy Index 06-05-2023	Policy & Procedure / Rules & Regulations / Policy Index	6/5/2023		3/2/2021
SOC-01 Hazardous Materials	Policy & Procedure / Rules & Regulations	5/15/2023	Department personnel, unless properly equipped and trained, shall not be deployed into areas that have	6/28/2019

1581	/ Policy & Procedure Documents		been contaminated, or face an immediate and substantial threat of contamination with a hazardous material.	
SOC-02 Bomb Threats / Explosive Incidents	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023	To establish and define the role of the Bomb Squad within the Division of Investigative Services-Fire and Explosion Investigation Unit (FEIU), and to establish guidelines for utilization and activation of their members.	6/28/2019
SOC-03 Emergency Planning	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023	To maintain and ensure the Department's compliance with Homeland Security Presidential Directive 8 (HSPD-8) with regards to emergency planning.	3/25/2020
SOC-03A Emergency Operations Center (EOC)	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/2/2021	To provide guidance to personnel regarding the activation and operation of the Department's Emergency Operations Center (EOC).	3/25/2020
SOC-03B Response to Emergency Situations	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023	To provide guidance for the Department's response efforts to public safety emergencies.	3/25/2020
SOC-03C Response to Civil Disturbances	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023	To provide guidance for the Department's response to civil disturbances.	3/25/2020
			The Department recognizes the Incident Command System (ICS) as a valid incident management system for use at the scenes of all	

1582 SOC-03D All Hazards Incident Command Framework	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023	emergency incidents. Regardless of the size or complexity of an incident, emergency responders must employ good management techniques to ensure an effective response and an efficient, safe use of resources. ICS helps emergency responders accomplish these goals. While ICS is normally associated with responses to emergency incidents, the Department further recognizes that ICS can be applied to a wide variety of incidents requiring Department response.	3/25/2020
SOC-03E Emergency and Continuity Plan Requirements	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023	In accordance with SOC-03 Emergency Planning, and SOC-03D All Hazards ICS Framework, the Department shall maintain written plans for responding to critical incidents including, but not limited to natural and man-made disasters, pandemics, civil disturbances, mass arrests, bomb threats, hostage/barricaded person situations, acts of terrorism, and other unusual incidents. These plans will follow standard Incident Command System (ICS) protocols and National Incident Management System (NIMS) which include functional provisions for: Command, Operations, Planning, Logistics and	1/29/2021

583			Finance/Administration.	
SOC-04 Lost / Missing Person Searches	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	Every incident involving a lost and/or missing person shall be treated as a potential emergency event that may require a rapid and coordinated response of specialized personnel and equipment. Members should understand that every lost and/or missing person incident has the potential of being or becoming a criminal investigation; members shall treat the scene of each incident as a potential crime scene. If the missing person is identified as a child age seventeen (17) or younger and there is evidence of abduction, the Amber Alert Coordinator shall be notified.	1/22/2021
SOC-04A AMBER Alert Activation	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	The Department shall initiate an AMBER Alert for cases of child abduction, where the child's life is in imminent danger of seriously bodily harm or death, and specific criteria supporting the AMBER Alert Activation have been met.	12/21/2020
SOC-05 Special Considerations	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	In accordance with international, federal, and state laws, the following are entitled to special considerations and/or immunities: *Diplomatic and consular officers; *Foreign Nationals; *Individuals requesting political asylum; *Military personnel;	6/22/2014

1584			and *Elected officials.	
SOC-06 Administration of Naloxone Hydrochloride (Narcan)	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	This policy shall establish protocol for Department members, in order to reduce life-threatening emergency of fatal opioid overdose, where medical professionals are not readily available, by administering naloxone hydrochloride. Department members shall assist any person who may be suffering from an opioid overdose. Department members trained in accordance with this policy shall make every reasonable effort, to include the use of naloxone combined with First Responder Training, to revive the victim of any apparent drug overdose.	7/29/2014
SOC-07 Domestic Abuse	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	The Department shall adhere to the Massachusetts Domestic Violence Law Enforcement Guidelines 2001.	4/23/2009
SOC-07A Domestic Abuse Arrest / Investigations	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023	The Department shall respond and investigate allegations of domestic abuse while ensuring the rights and safety of all those involved.	4/23/2009
SOC-07B Domestic Abuse Involving Members	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	The Department shall ensure that all reports of alleged domestic abuse by members are thoroughly investigated. The Department shall respond and investigate allegations of domestic abuse while ensuring	6/17/2013

585			the rights and safety of all those involved.	
SOC-07C Abuse of Children / Disabled / Elderly	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	The Department shall investigate all allegations regarding the abuse of children, the disabled, and the elderly, to ensure the safety and rights of all those involved.	7/22/2014
SOC-08 Missing-Abandoned-Runaway Children	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	The Department shall thoroughly investigate all reports of missing children. Every child reported missing to the Department will be considered at risk until significant information to the contrary is confirmed. Incidents involving missing, abandoned and/or a runaway child shall be treated as a potential emergency event that may require a rapid and coordinated response of specialized personnel and equipment. Every lost and/or missing child incident has the potential of being or becoming a criminal investigation; members shall treat the scene of each incident as a potential crime scene.	1/22/2021
SOC-09 Terrorism / WMD Incidents	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	The preservation of life and the prevention of injury shall be recognized as high priorities in responding to terrorist incidents, including those involving Weapons of Mass Destruction.	6/28/2019
SOC-10 Clandestine Drug Laboratory Response	Policy & Procedure / Rules & Regulations / Policy &	7/8/2022	To define the role of the Clandestine Laboratory Enforcement Team (CLET) and establish guidelines for the utilization and	6/28/2019

1586	Procedure Documents		activation of team members.	
SUP-01 Jurisdiction_Mutual Aid	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023	To define the role of the Clandestine Laboratory Enforcement Team (CLET) and establish guidelines for the utilization and activation of team members.	4/23/2009
SUP-03 Media Relations	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023	The Department shall provide the media and the public with information on Department operations and administration, ensuring that individual rights are protected.	4/23/2009
SUP-04 Employee Assistance Unit	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/5/2021	The Department has a responsibility to ensure the safety of our employees and to contribute to their psychological and physical well-being. The Department shall offer to employees and their families, professional assistance, training, peer counseling, and professional referrals.	7/11/2011
SUP-04A Critical Incident Stress Management Team	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	2/17/2023		2/17/2023
SUP-05 State Police Chaplain Corps	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023	The Department has a responsibility to ensure the safety of our employees and to contribute to their psychological and physical well-being. The Department shall offer to employees and their families, professional assistance, training, peer	4/10/2019

1587			counseling, and professional referrals.	
SUP-06 Binding Written Agreements	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	All Memorandum of Understandings, Mutual Aid Agreements, or any other type of binding written agreements (collectively referred to as "MOUs") between the Department and outside organizations, including any state or federal agency, shall only be authorized and signed by the Colonel/Superintendent.	4/23/2009
SUP-12 Office of The Ombudsman	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	The Ombudsman Program provides a confidential, neutral, and informal process to help resolve work-related issues. It is a dispute resolution system that offers employees formal and informal options for addressing work-related problems and concerns. Although the program is an alternative channel of communication, it is designed to complement, not replace or circumvent the Department's formal resolution options.	7/11/2011
TOP-01 Special Operations Command and Control	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	The Ombudsman Program provides a confidential, neutral, and informal process to help resolve work-related issues. It is a dispute resolution system that offers employees formal and informal options for addressing work-related problems and concerns. Although the program is an alternative channel of communication, it is	6/14/2018

			designed to complement, not replace or circumvent the Department's formal resolution options.	
TOP-02 Special Tactical Operations Team	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	To establish and define the role of the Special Tactical Operations Team within the Division of Field Services-Special Operations and establish guidelines for activation and utilization of their resources.	6/17/2013
TOP-03 Crisis Negotiation Team	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023	To establish and define the role of the Crisis Negotiation Team within the Division of Field Services-Special Operations and establish guidelines for activation and utilization of their resources.	6/17/2013
TOP-04 Mounted Unit	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023	To establish the role of the Mounted Unit within the Division of Field Services-Special Operations and establish guidelines for activation and utilization of their resources.	6/17/2013
TOP-05 Canine Unit	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023	To establish and define the role of the Canine Unit within the Division of Field Services-Special Operations and establish guidelines for activation and utilization of their resources.	6/17/2013
TOP-06 Underwater Recovery Team	Policy & Procedure / Rules & Regulations / Policy &	5/15/2023	To define the role of the Underwater Recovery (Dive) Team within the Division of Field Services-Special Operations and	6/17/2013

1589	Procedure Documents		establish guidelines for activation and utilization of their resources.	
TOP-07 Air Wing	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023	To define the role of the Air Wing within the Division of Homeland Security and Preparedness and establish guidelines for activation and utilization of their resources.	6/14/2018
TOP-07A Small Unmanned Aircraft Systems (UAS)	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	To define the operation of small Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) within the Department of State Police.	6/28/2019
TOP-08 Marine Unit	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	To define the role of the Marine Unit within the Division of Homeland Security and Preparedness and establish guidelines for activation and utilization of their resources.	6/14/2018
TOP-09 Incident Management Assistance Team	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	To define the role of the Incident Management Assistance Team (IMAT) within the Division of Homeland Security and Preparedness and establish guidelines for activation and utilization of its resources.	6/28/2019
TOP-10 Special Emergency Response Team	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	To establish and define the role of the Special Emergency Response Team within the Division of Field Services-Special Operations and establish guidelines for activation and utilization of their resources.	6/17/2013

590 TOP-11 Emergency Management Unit	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	To establish and define the role of the Emergency Management Unit within the Division of Field Services-Special Operations and establish guidelines for activation and utilization of their resources.	6/17/2013
TOP-12 Motorcycle Unit	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	To establish and define the role of the Motorcycle Unit within the Division of Field Services-Special Operations and establish guidelines for activation and utilization of their resources.	7/22/2014
TOP-13 Behavioral Observation and Suspicous Activity Recogition Unit (BOSAR)	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023		12/1/2021
TRF-01 Mission Goals and Objectives	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023	All members are responsible for facilitating the safe and expeditious flow of traffic.	1/22/2021
TRF-02 Patrol	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/5/2021	The Department shall provide twenty-four (24) hour a day patrol coverage of state and interstate highways, as well as other areas of primary jurisdiction. The Department shall also be available to assist other agencies when required.	1/22/2021
TRF-03 Selective Traffic Enforcement	Policy & Procedure / Rules & Regulations / Policy &	5/15/2023	The Department shall use special enforcement patrol duties as an effective technique to meet highway traffic	1/22/2021

591	Procedure Documents		safety goals and objectives.	
TRF-04 Motor Vehicle Pursuits	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	12/1/2021	The Department shall use special enforcement patrol duties as an effective technique to meet highway traffic safety goals and objectives.	1/25/2021
TRF-04A Foot Pursuits	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	Members shall continuously evaluate all circumstances surrounding a pursuit. If the degree of danger to the public, the pursuing officer(s), and/or member(s) is greater than the necessity for immediate apprehension, a pursuit should not be initiated, or, if in progress, should be terminated.	1/25/2021
TRF-05 Traffic Incident Management	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023	The Department shall use Traffic Incident Management protocols to minimize the congestion and delay caused by highway incidents. Traffic congestion causes safety concerns due to the increased risk of secondary crashes. Every effort should be made to minimize this risk, in addition to the impact to public safety and the inconvenience to motorists of the Commonwealth.	1/22/2021
TRF-07 Motor Vehicle Stops	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/5/2021	Necessary precautions shall be taken for every motor vehicle stop to ensure the safety of all. Members shall use these guidelines as well as their training and experience to determine specific actions for each situation.	1/22/2021

1592 TRF-08 Traffic Citations	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/3/2021	Traffic citations shall be issued in accordance with Policy and Procedure ADM-04 State Police Authority and Massachusetts General Law (MGL) c. 90C.	1/22/2021
TRF-09 Towing	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	To establish and define guidelines for State Police Officers engaged in towing vehicles.	1/29/2021
TRF-10 Vehicle Inventory	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	Any vehicle towed, or in the custody of the Department, shall be inventoried and properly documented in order to protect: *The vehicle and its contents; *The Department and tow company against false claims of lost, stolen, or vandalized property; and * The member(s) and the public from dangerous items that might be in the vehicle.	1/21/2021
TRF-11 Automatic License Plate Recognition	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	6/27/2023	The availability and use of the Automatic License Plate Recognition (ALPR) System provides opportunities for enhancing the productivity and effectiveness of law enforcement agencies. The ALPR System also provides opportunities to increase public and officer safety. The Department shall only utilize the technology in furtherance of official and legitimate law enforcement operations and public safety. All Department Employees	1/22/2021

1593			shall abide by the guidelines set forth herein when using the ALPR System.	
TRF-12 Crash Investigations	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/5/2021	To establish guidelines for traffic crash reporting and investigations	1/22/2021
TRF-14 OUI	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/23/2023	To promote traffic safety through the detection, arrest and prosecution of subjects operating a motor vehicle while under the influence of alcohol and /or drugs. Members establishing probable cause of a subject operating a motor vehicle under the influence of alcohol and/or drugs should effect the arrest of said subject unless articulable extenuating circumstances prevent taking the subject into custody and necessitate an alternative means of enforcement at the time of the identified offense(s).	1/22/2021
TRF-14B Preliminary Portable Breath Test Devices	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	To provide guidance for the proper use, documentation, and maintenance of Preliminary Breath Test (PBT) instruments.	1/22/2021
TRF-15 Sobriety Checkpoints	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	When utilized, Sobriety Checkpoints shall be conducted in conformance with judicial guidelines.	1/22/2021
	Policy & Procedure /		The Department shall use speed measuring	

594 TRF-16 Speed Measuring Devices	Rules & Regulations / Policy & Procedure Documents	5/15/2023	devices as part of the strategy to reduce motor vehicle crashes and enhance public safety within the Commonwealth.	1/22/2021
TRF-17 Emergency Roadblocks	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	At times, situations arise which may necessitate the utilization of an emergency roadblock. To ensure the safety of the public and Department members, many factors have to be considered prior to implementation of a roadblock. Only Commissioned Officers may approve and authorize the implementation of an emergency roadblock.	1/22/2021
TRF-20 Department Vehicle Crash	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	The Department shall document, within the Records Activity Management System (RAMS), all Department vehicle crashes in accordance with this policy. The Department shall objectively investigate all vehicle crashes, in order to ensure that each crash investigation reflects the Department's commitment to impartiality and integrity.	1/29/2021
TRF-21 Tire Deflation Devices	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	The Department may use tire deflation devices in specific circumstances to reduce the speed and duration of pursuits in order to reduce the risk of injury to persons and/or damage to property.	1/22/2021
	Policy &		The Department may authorize escorts or	

1595 TRF-22 Escorts, Relays and VIP_Dignitary Security	Procedure / Rules & Regulations / Policy & Procedure Documents	7/8/2022	relays to provide added security, expedite the delivery of special items, and ensure the safe and efficient movement of traffic.	1/22/2021
TRN-01 Training Administration	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023	The Department shall provide training that will develop the skills necessary for the safe, professional and effective performance of its personnel, and that is designed to promote and maintain the professionalism and operational readiness of the Department. The Department shall ensure that all employees successfully complete compulsory training as required by law and the Colonel/Superintendent.	1/22/2021
TRN-02 Recruit Training	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023	Prior to assuming duties as a sworn State Police Trooper, recruits shall be assigned to, and satisfactorily complete a recruit training class. This class shall be held at the State Police Academy and fulfill the requirements as prescribed by Massachusetts General Laws and the Colonel/Superintendent.	1/22/2021
TRN-03 Field Training Program	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023	The Department shall provide a Field Training Program to transition from the controlled learning environment of the Academy to the responsibilities and duties of a State Trooper.	1/22/2021
	Policy &		The Department recognizes the necessity of continuous education and training in order to	

596 TRN-04 Professional Development	Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023	maintain and enhance the knowledge, abilities, and skills of its employees. This shall be accomplished, in part, through an ongoing professional development program to include regular in-service training.	1/22/2021
TRN-05 State Police Cadet Program	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	11/22/2022		11/22/2022
UOF-01 Use of Force	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	Members are authorized to use only that force which is objectively reasonable, in accordance with all applicable federal and state laws and regulations and the contents of this policy to: * Effect the lawful arrest or detention of a person; *Prevent the escape from custody of a person; or *Prevent imminent harm, and the amount of force used is proportionate to the threat of imminent harm.	1/22/2021
UOF-02 Use of Lethal Force Response	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/16/2023	The Department shall immediately respond to the scene and conduct an investigation when a use of force results in: *A death; *Serious bodily injury; and/or *Any reportable discharge of a firearm per UOF-03 Reports.	1/22/2021
UOF-03 Use of Force Reporting	Policy & Procedure / Rules & Regulations / Policy &	5/15/2023	All incidents involving the use of force shall be documented. Members shall adhere to the Duty to Intervene and Report mandates of General	1/22/2021

1597	Procedure Documents		Order UOF-01, Use of Force.	
UOF-04 Use of Force - Equipment	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023	Members on duty shall carry and use only Department issued use of force (UOF) equipment for which they have received Department approved training and maintain a current certification.	1/22/2021
UOF-05 Use of Force Training	Policy & Procedure / Rules & Regulations / Policy & Procedure Documents	5/15/2023	The Department shall provide training and instruction to every member to become proficient in the use of issued weapons and control techniques. All members shall successfully complete approved training and shall qualify with weapons and techniques prior to use. Training protocols shall adhere to, or exceed, applicable federal and state laws and regulations for members to become, and remain in good standing as law enforcement officers. The Department's training protocols shall include substantive instruction on the agency's use of force (UOF) policies and procedures, de-escalation techniques, and related legal updates.	1/22/2021
UOF-06 Electronic Control Weapons	Policy & Procedure / Rules & Regulations / Policy & Procedure	5/15/2023	The Department shall ensure proper guidance and direction on the use of Electronic Control Weapons (ECWs). Only those Department members who have successfully completed the Department's initial ECW training and	1/22/2021

1598	Documents		subsequent in-service ECW training are authorized to use an ECW.	

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**ADM-01**
Subject:	
Oath of Office	

Policy

All sworn members of the Department of State Police shall take and affirm an Oath of Office prior to the initial performance of duties.

Oath of Office

I do solemnly swear that I will bear true faith and allegiance to the Commonwealth of Massachusetts, and will support the Constitution thereof, so help me God.

I do solemnly swear and affirm that I will faithfully and impartially discharge and perform all the duties incumbent on me as a Massachusetts State Police Trooper: according to the best of my abilities and understanding, agreeably, to the rules and regulations of the Constitution, and the laws of this Commonwealth, so help me God.

I do solemnly swear that I will support the Constitution of the United States.

References: MGL c.22C, §15;
MPAC: 26.0.1.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**ADM-02**

Subject:

Department Mission Statement

Mission

As the principal state-wide law enforcement agency in the Commonwealth, the Massachusetts State Police, in partnership with local communities, shall provide for the public safety by providing quality policing directed at achieving safer roadways and reducing crime through investigations, education and patrol services, and by providing leadership and resources during natural disasters, civil disorders and critical incidents.

Policy

The Department of State Police, in cooperation with the Executive, Legislative, and Judicial branches of government, shall ensure that justice in a free society is perpetually prevalent.

Organizational Values

The value statements of the Massachusetts State Police are:

- Maintenance of the highest standard of integrity and ethics;
- Excellence and teamwork in the performance of duty;
- Protection of Constitutional Rights;
- Problem solving for continuous improvement;
- Continuous planning for the future; and
- Performing public service and law enforcement tasks so as to provide leadership to the police profession.

References: Rules and Regulations 2.0;
MPAC: 11.1.0.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**ADM-04**

Subject:

State Police Authority

Policy

Within the Commonwealth, sworn members shall exercise all the powers of police officers as authorized by law and exercise professional discretion when appropriate.

Limits of Authority

No member may be used or called upon for service at any industrial dispute unless actual violence has occurred therein, and then only by written order of the Governor.

Members shall not exercise police powers on a reservation or other property of the United States of America unless requested by the person in charge of the reservation or property.

No member shall serve civil process.

Discretion

When Rules and Regulations, Policy and Procedure, other Orders or Directives, fail to provide specific guidance, members shall exercise professional discretion that may be based upon:

- Training, experience, common sense;
- Principles, values, ethics;
- Advice from supervisors, senior officers; and
- Professionally accepted standards.

Discretionary measures may include:

- Application for complaint;
- Verbal or written warnings;
- Referral to other divisions, departments, or agencies;
- Guidance from the Attorney General/District Attorney; and
- Informal resolution.

References: MGL c.1, § 7, c.22C, § 10, § 50;
40 USC §318;
MPAC: 1.1.0, 2.1.1, 16.3.0, 41.4.4, 74.2.1.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**ADM-05**
Subject:	
Organizational Structure	

Policy

The Department's organizational structure is arranged in a manner that simplifies the direction, coordination, and control of personnel.

Organizational Structure

The Superintendent does hereby establish the following operational Divisions for the effective and efficient delivery of services:

- Division of Field Services;

The mission of the Division of Field Services (DFS) is to: provide uniformed policing and patrol service to the citizens of, and visitors to, the Commonwealth in order to facilitate motor vehicle crash and fatality reduction utilizing proactive enforcement and education to ensure the safe and expeditious flow of traffic; deter, interdict, apprehend and prosecute those engaged in criminal activity; provide primary policing and law enforcement services to the Massachusetts State House, Massachusetts Department of Conservation and Recreation, Massachusetts Port Authority, Massachusetts Department of Transportation and Massachusetts Water Resource Authority; and to provide special and tactical resources in order to assist municipal law enforcement agencies in effectively responding to public safety emergency incidents or events throughout the Commonwealth.

- Division of Investigative Services;

The mission of the Division of Investigative Services (DIS) is to: reduce criminal activity in the Commonwealth in cooperation with local and federal law enforcement agencies by gathering, analyzing and reporting on the type, manner and location of criminal activity within the Commonwealth; monitor the activities and associations of individuals engaging in organized crime; investigate criminal acts for the purpose(s) of identifying, apprehending and prosecuting perpetrators; apprehend fugitives from justice, and provide executive protection.

Organizational Structure, continued

- Division of Standards and Training;

The mission of the Division of Standards and Training (DST) is to improve the quality of the services provided by the Department ensuring the integrity and competence of its operations. This mission shall be accomplished through the continual training and education of Department members; the investigation, and when deemed appropriate, the prosecution of Department personnel misconduct; and the regular inspection of Department operations and facilities. The Division shall work cooperatively with local and federal law enforcement agencies, as well as the general public, providing training and education in public safety and law enforcement related matters.

- Division of Homeland Security and Preparedness;

The mission of the Division of Homeland Security and Preparedness (DHS) is to lead the Department's criminal intelligence, counterterrorism, cybersecurity, emergency preparedness, and emergency response efforts, employing an intelligence-led policing approach to sustaining, enhancing and coordinating the Department's statewide capabilities to prepare for, protect against, investigate, respond to and recover from any criminal, terrorist, natural or manmade hazards or threats.

- Division of Administrative Services;

The mission of the Division of Administrative Services (DAS) is to provide the material resources and logistical support necessary for the Department to fulfill its mission by: preparing a complete and relevant budget; procuring and maintaining necessary equipment and facilities; and providing services for supporting the physical, financial and morale needs of Department personnel.

- Forensic Services Division.

The mission of the Forensic Services Division (FSD) is to provide forensic services to criminal justice agencies in the Commonwealth by supplying on-scene technical assistance to law enforcement agencies statewide, performing laboratory analysis of scientific evidence in connection with criminal cases, and offering expert scientific testimony in state and federal court proceedings.

Organizational Charts

Organizational charts graphically depict organizational entities, levels of command, lines of authority, and positions established for the duties of personnel.

The charts shall be:

- Updated continually to reflect Organizational change(s) in Command and/or reporting;
- Reviewed by each Division Commander prior to the next fiscal year;
- Revised through the Office of the Superintendent; and
- Be accessible to the public upon submission of record request.

Subject:	Number:
Organizational Structure	**ADM-05**

Accountability

Each employee is accountable:
- For the use of their authority delegated to others; and
- For the performance of any personnel under their control.

Chain of Command

The chain of command is the extension of authority and responsibility from the Colonel/Superintendent down to the level of execution.

Responsibility is accompanied by commensurate authority.

The chain of command for sworn members, in order of descending rank, shall be:
- Colonel/Superintendent;
- Lieutenant Colonel/Deputy Superintendent;
- Lieutenant Colonel;
- Major;
- Detective Captain;
- Captain;
- Detective Lieutenant;
- Lieutenant;
- Sergeant; and
- Trooper - The senior Trooper is in command, when necessary.

Command

Each organizational entity shall be:
- Under the direct command of only one supervisor.

Each employee shall be:
- Accountable to only one supervisor at any given time; and
- Bound by the chain of command that is applicable to their position.

Supervisory ratio must be:
- Adequate to provide guidance and control, as determined by the Colonel/Superintendent.

Ranking personnel shall:
- Assume line control outside their own organizational entity when failure to do so would seriously endanger the Department's:
  - Ability to maintain law and order; and
  - Public image.

References: Rules and Regulations Article 3;
MPAC: 11.1.1, 11.1.2, 11.2.1, 11.3.1, 11.3.2.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**ADM-06**

Subject:

Command Staff Responsibilities

Policy

The Command Staff is responsible for the administrative and operational control of the Department. Each member of the Command Staff shall maximize their involvement in the operations of the Department to deliver the highest level of public safety services to the public and other law enforcement entities.

Definition

The Command Staff shall include the following ranks:

- Colonel/Superintendent;
- Lieutenant Colonel/Deputy Superintendent;
- Lieutenant Colonel;
- Major; and
- Civilian Members of the Command Staff:
  - Chief Administrative Officer
  - Chief Science Officer.

Responsibilities

Position	Duties
Colonel/Superintendent	• Act as the Chief Executive Officer of the Department; • Assume full authority over the organization, administration and discipline of the Department; and • Promulgate all rules, regulations, policies, procedures, orders and directives.
Lieutenant Colonel/Deputy Superintendent	• Act as the Chief Operating Officer of the Department; and • Assume command of the Department as assigned and during the absence of, or when so designated by the Colonel/ Superintendent.
Lieutenant Colonel	• Act as the Chief Operating Officer of a Division.
Chief Administrative Officer	• Act as the Chief Administrative Officer and Division Commander of the Division of Administrative Services.
Chief Science Officer	• Act as the Chief Operating Officer of the Forensic Services Division.
Major	• Serve as a Troop Commander or other organizational unit head as directed by the respective Division Commander.

Meetings

Staff meetings shall be conducted to encourage and support the exchange of information. This may include a weekly staff meeting between the Colonel and all Divisions. Information from these meetings shall be distributed to all affected personnel as directed by the Colonel/Superintendent.

References: MGL c.22C, §2, §3;
MPAC: 12.1.2;
Rules and Regulations 3.1, 3.2, 3.3, 3.6.2.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

1607

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**ADM-07**
Subject:	
Written Directives, Schedules and Forms	

Policy

The Department shall provide administrative direction and operational guidance through an internal written directive process. Written directives shall be formatted, indexed and accessed according to the guidelines set forth in this policy unless otherwise directed by the Office of the Superintendent.

Written Directive

Directive	Approving Authority	Purpose
General Order	Superintendent	• Codify the policies and procedures of the State Police.
Rules & Regulations	Superintendent	• Regulate the governance of the State Police.
Personnel Order	Superintendent	• Assignments • Appointments • Discipline • Transfers • Discharges • Commendations
Special Order	Superintendent	• Specific instructions for specific personnel; and/or • Dissemination of information relative to a particular topic or incident.
Superintendent's Memorandum	Superintendent	• Formal or informal clarification or inquiry.
Division Commander's Order	Division Commander	• Administrative order issued for members under their command.
Administrative Notice	Superintendent/ Deputy Superintendent	• To inform members about general issues (crime, training, law updates, etc.); and/or • Address item(s) not covered by the above directives.
Standard Operating Procedures	Deputy Superintendent	• Procedures specific to the operations of individual sections/units.
Academy Training Bulletin	DST Division Commander	• To provide information related to specific current training topics.

Responsibilities for Written Directives

Position	Duties
Colonel/ Superintendent	• Approve and sign applicable written directives; and • Establish a Policy Review Committee.
Deputy Superintendent	• Review and approve SOP's.
Policy Review Committee	• Ensure that each Department Rule & Regulation, General Order and SP Form is reviewed at least annually, revised as needed; and • Consider suggestions/recommendations regarding the revision or creation of a General Order and/or SP Form:
Human Resources	• Ensure all Personnel Orders are posted and archived accordingly.
Division Commanders	• Approve and sign Division Commander Orders; • Ensure all Division Commander's Orders are posted and archived accordingly; • Review all Section/Unit SOP's annually; • Return SOP's approved by the Deputy Superintendent to the Section/Unit Commander for Section/Unit promulgation; • Assign a Commissioned Officer to review Division Commander's Orders annually; and • Assign a Commissioned Officer to the Departmental Policy Review Committee as directed by the Office of the Superintendent.
Strategic Planning Section	• Post approved written directives, excluding Division Commander's Orders and Personnel Orders on PowerDMS and/or DocuShare; and • Archive all written directives, excluding Division Commander's Orders and Personnel Orders.
Legal Section	• Review written directives as directed by the Office of the Superintendent.

Written Directive Formatting

Policy & Procedure
- Shall be indexed with prefix denoting administrative code, title and effective date.

Rules & Regulations
- Shall be indexed with effective date, number and subject (appendix or article).

Standard Operating Procedures
- Shall be indexed by the respective Section/Unit Commander to include effective date, numeric order, subject and review date.

Other written directives
- Shall be indexed by directive type and include/denote the issuing entity, effective date, numeric order by year (excepting General Orders) and subject matter.

As applicable, review/revision and effective dates will be updated and shall be signed by the person with authority to issue such directive.

Formatting will be consistent with all other directives posted on PowerDMS and/or DocuShare. The Strategic Planning Section can provide assistance with formatting but is not responsible for content creation unless directed by the Office of the Superintendent.

Publication

Department written directives, with the exception of Section/Unit SOP(s) shall be published on PowerDMS and/or DocuShare.

Section/Unit Commanders shall be responsible for the distribution and access to Section/Unit SOP(s) for personnel under their command.

If applicable, Troop/Section Commanders shall ensure that Department bulletin boards are maintained with current directives and are accessible to all personnel.

Distribution / Receipt and Familiarization

The Colonel/Superintendent shall ensure written directives are properly distributed and posted.

It is the responsibility of each sworn and civilian employee to read and familiarize themselves with promulgated directives. Sworn and civilian employees shall:
- Read promulgated directives within one week of distribution or upon return to duty for members on approved leave;
- Familiarize themselves with Policy & Procedures and Rules & Regulations as issued;
- Access PowerDMS and electronically sign an acknowledgment of receipt and review of all written directives posted to PowerDMS;

Distribution / Receipt and Familiarization, continued

- Sign appropriate Signature Receipt Form to acknowledge receipt and review of all other written directives (Each Division shall maintain a copy of signature sheets acknowledging assigned employees have read issued directives); and
- Civilian employees shall direct questions on applicability of specific written directives to their immediate supervisor.

Duration

All General Orders, Personnel Orders, and Superintendent's Memorandums shall:

- Be reviewed on an annual basis as applicable; and
- Remain in effect until:

Rescinded by the Colonel/Superintendent; or
Superseded by another General Order, Personnel Order, or Superintendent's Memorandum.

Division Commander's Orders shall:

- Be reviewed on an annual basis; and
- Remain in effect until:

Rescinded by the Division Commander or Colonel/Superintendent; or
Superseded by another Division Commander's Order or General Order promulgated by the Colonel/Superintendent.

All other written directives are valid for one (1) year, unless rescinded. New directives may be issued at any time. These directives shall be reviewed at the end of one (1) year by the issuing authority prior to re-issue.

The Strategic Planning Section shall facilitate the annual policy review process, including, but not limited to, establishing the review schedule and maintenance of the review records.

Changes

All written directives shall be amended to coincide with the terms of current Collective Bargaining Agreement(s), state and federal laws, and including Executive Orders.

When a negotiated labor agreement is ratified by all parties, the Colonel/Superintendent or designee, shall:

- Obtain a written, signed copy of the labor agreement; and
- Review and amend, if necessary, all written directives and procedures to coincide with the terms of the labor agreement.

The Office of Employee Relations shall disseminate information relative to a new labor agreement, including modifications to existing agreements, to managers and supervisors of bargaining unit employees.

Members are encouraged to make suggestions and recommendations to revise or create written directives. Such suggestions/recommendations shall be written and forwarded, through channels, to the Office of the Superintendent-Strategic Planning Section for consideration by the Department Policy Review Committee.

Requesting Written Directives

To obtain a copy of a written directive, members shall access PowerDMS and/or DocuShare. If unable to access PowerDMS and/or DocuShare, members shall consult their commanding officer who shall make the request through channels to the Strategic Planning Section.

Archives

Department written directives, excluding Division Commander's Orders and Personnel Orders, shall be maintained by the Office of the Superintendent-Strategic Planning Section, including the signed "master copy".

Division Commanders and the Human Resources Section shall maintain the signed "master copy" of their Division Commander's Orders or Personnel Orders.

"SP" Forms

The Policy Review Committee shall consider suggestions/recommendations forwarded, in writing, through channels to the Office of Superintendent-Strategic Planning Section concerning the creation of a new or revision to an existing Department "SP" Form; and

Station/Section/Unit Forms, strictly used within their station/section/unit for Department business and not forwarded to any outside entities, are not under the purview of the Strategic Planning Section and shall not be issued a Departmental "SP" number.

Exclusive Directives

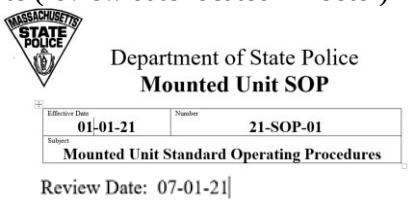
Commanding Officers may create written directives for the administration of their respective entities. Directives shall be filed with their appropriate Division Commander and shall remain in effect for one (1) year unless:

- Rescinded; or
- The directive conflicts with a Division Commander Order or General Order.

Standard Operating Procedures (SOP)

Section/Unit Commanders shall:

- As applicable, create and maintain an internal SOP specific to their function to include effective date, numeric order, subject and review date (review date located in footer) formatted similar to example below;


Department of State Police
Mounted Unit SOP

Effective Date	Number
01-01-21	21-SOP-01
Subject: Mounted Unit Standard Operating Procedures	

Review Date: 07-01-21

  - Above template for SOP's can be obtained from the Strategic Planning Section;
  - Sections/Units with SOP's that are lengthy may utilize alternative formatting provided the cover sheet includes the above information;
- Forward a copy through channels to the Deputy Superintendent for approval;
- Upon approval, provide Section/Unit members with a copy of the approved SOP via Section/Unit Commander discretion of manual or electronic distribution, documenting distribution/receipt within RAMS/ACISS;
- Review SOPs annually and submit any revised SOP's through channels to the Office of the Superintendent for review/approval prior to promulgation; and
- Annually update the review date to document the review and update the effective date upon the implementation of any changes to said SOP.

Master Vacation Schedule

Each Troop/Station/Section/Unit Commanding Officer shall:

- Submit through channels the Master Vacation Schedule for all sworn and civilian employees under their command to their Division Commander on or before February 14th of each year; and
- Ensure that all sworn and civilian employees have selected vacation week(s) according to their collective bargaining agreement.

Division Commanders shall:

- Retain submitted Master Vacation Schedules for the current year for all sworn and civilian employees under their command.

Division of Administrative Services / Human Resources Section: shall:

- Post a blank copy of the Master Vacation Schedule to PowerDMS-Department Forms prior to January 1st.

References M.G.L. c. 22C, § 2, § 3;
MPAC: 12.2.1, 12.2.2, 24.1.2, 26.1.8.
20-SM-07 Establishment of Departmental Policy Review Committee

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**ADM-08**
Subject:	
Strategic Planning	

Policy

In order to provide effective management and planning, the Department shall:

- Establish, review and revise a Multi-Year Plan;
- Establish goals and objectives for the Department and each Division;
- Continuously review, revise and track the progress of established goals and objectives;
- Make established goals and objectives available to all agency personnel;
- Annually review and revise written directives; and
- Maintain a grant application process.

Division Goals & Objectives

Each Division will develop goals and objectives that are based upon and designed to promote, enhance and achieve:

- The overall mission and organizational values of the Department as stated in ADM-02 State Police Mission and Policy;
- Division mission(s) as stated in ADM-05 Organizational Structure;
- Interoperability of Divisions where applicable; and
- The Department's Multi Year Plan.

Division Commanders shall meet, at least annually, with the Office of the Superintendent to review, evaluate, and update the stated goals and objectives of their respective Division.

Progress Review

The Colonel may request goal and objective progress review reports from Divisions at any time. Additionally, prior to September 30th of each year, each Division Commander shall submit a *written program evaluation* of their Divisional goals and objectives to assist the Office of the Superintendent in conducting a formal review assessing progress towards achieving the stated goals and objectives.

Division Goals & Objectives, continued

Prior to November 30st of each year, each Division Commander shall submit, in writing, to the Office of the Superintendent a Divisional Goals and Objectives report.

The Divisional Goals and Objectives report shall:

- Enumerate the goals and objectives for the Division;
- Indicate the progress that has been made towards achieving the goals and objectives for the Division; and
- Address unrealized goals/objectives and plan for achievement where applicable.

Division Planning Officer

Each Division Commander shall assign a Commissioned Officer as the Division's Planning Officer who shall:

- Coordinate the development, implementation and review of the Division's goals and objectives;
- Work with the Division's Station/Section/Unit Commanders to:
  - Establish the goals and objectives for the respective entities;
  - Identify the resources and initiatives necessary to achieve these goals and objectives; and
  - Provide to the Division Commander a listing of these goals and objectives and the resources and initiatives necessary to achieve them.
- Act as a point of contact for Station/Section/Unit/Commanders within their Division regarding technological advancement, equipment procurement, and other programs and initiatives that may be eligible for, acquired through, and/or developed and/or enhanced by grant funding; and
- Act as the Project Administrator, as prescribed in ADM-08A Grant Approval Process to:
  - Review, track and oversee a specific funding request/project;
  - Complete required quarterly and annual reports;
  - Maintain oversight on the Division's grant program operations and reporting;
  - Assist employees submitting grant proposals with obtaining the required Divisional signatures on the SP 426 Grant/Agreement Approval Request;
  - Work directly with the Strategic Planning Section and Fiscal Section throughout the grant application process; and
  - Provide the appropriate Division, Station/Section/Unit Commanders, with grant application progress updates.

Department Annual Goal and Objective Report

Utilizing and compiling the Divisional Goals and Objectives reports submitted by each Division to the Office of the Superintendent prior to November 30th each year, the Strategic Planning Section shall generate the Department's Annual Goal and Objective Report. The Department's Annual Goal and Objective Report will enumerate the goals and objectives for the agency and for each major organizational component within the agency.

On or prior to December 30th of each year, Strategic Planning will forward the Annual Goal and Objective Report to the Colonel for review. Upon approval by the Colonel, the final Annual Goal and Objective Report shall be posted on PowerDMS.

Strategic Planning and Analysis Section

The Strategic Planning and Analysis Section shall:

- Report to the Office of the Superintendent;
- Assist the Command Staff with the Department's administration and control through planning, research, and coordination;
- As prescribed in ADM-07:
  - Assist Divisions with the revision, editing and chain of command review of current and proposed written directives (excluding Division Commander's Orders and Personnel Orders);
  - Facilitate the annual review of MSP Policies, Rules & Regulations in accordance with the established schedule;
  - Post promulgated written directives (excluding Division Commander's Orders and Personnel Orders) on PowerDMS;
  - Archive all written directives (excluding Division Commander's Orders and Personnel); and
  - Maintain the SP Forms management process, including design, inventory, archiving and promulgation;
- Compile Divisional Goal and Objective reports, prepare and submit the Department's Annual Goal and Objective Report to the Colonel/Superintendent for approval and promulgation on PowerDMS;
- Research and forward to Division Commanders and the designated Divisional Planning Officers any Notices of Funding Opportunity for which the Department is eligible;
- Instruct and assist members and the Divisional Planning Officers during the grant application process;
- Provide research regarding Departmental initiatives when requested; and
- Research emerging technologies and trends.

Subject:	Number:
Strategic Planning	**ADM-08**

References: ADM-02 State Police Mission and Policy;
ADM-05 Organizational Structure;
ADM-07 Written Directives;
ADM-08A Grant Approval Process;
Multi-Year Plan;
SP 426 Grant/Agreement Approval Request;
MPAC: 12.2.1, 15.1.3, 15.2.1, 15.2.2.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**ADM-08A**
Subject:	
Grant Approval Process	

Policy

Whenever Department employees seek to obtain services and/or funding through private, public (including state or federal) entities; or to acquire or transfer equipment from an outside entity, employees shall adhere to the procedures contained herein .

Definitions

Grant requests can be any of the following:

- *Grant*: An award of financial assistance from an external entity where no "substantial involvement" is anticipated between the awarding entity and the Department during performance of the agreed upon activity.
- *Cooperative Agreement*: An agreement of financial assistance where there is "substantial involvement" anticipated between an external entity and the Department during the performance of an agreed upon activity. Cooperative agreements are often non-cash agreements involving services provided to or by the Department.
- *Interagency Service Agreement* (ISA): An agreement between the Department and a Massachusetts state entity, which is committing funds for a specific program.
- *Equipment Acquisition Agreement*: Agreements where the Department shall receive equipment to provide services, perform a specific function, or use within its operations.

Director of Federal Grant Initiatives: A member from the Division of Administrative Services who is responsible for monitoring the grants request process and assisting members in grant research, application, and submission.

Grants Unit: A unit within the Department's Fiscal Section under the Division of Administrative Services, which is responsible for the grant fiscal oversight process through the Office of the State Comptroller and ensures the timely submission of expenditure documentation as necessary to ensure compliance with grant award(s).

Match Funds: The portion of funds that the Department shall provide to supplement the funding agency's contribution. The match is usually a percentage of the project's total budget.

Project Administrator: An employee appointed by their Division Commanderto oversee a specific request/project and is responsible for the completion of all quarterly and annual reports.

Definitions, continued

SP 426 Grant/Agreement Approval Request Form: A form to be completed by employees requesting approval to initiate the application process for any services, funding, and/or equipment acquisitions.

Process

Unless prior written approval has been granted from the Colonel/Superintendent, employees shall not:

- Enter into any grants, cooperative agreements, or interagencyservice agreements; or
- Submit an application, or solicit or accept funding and/or equipment from any outside entities.

Equipment

Project Administrators shall comply with ADM-30 Asset Management when receiving equipment through a grant request.

Grants Review Committee

Requests for grant funding shall be reviewed by the following Department members prior to submission to ensure they align with departmental goals and objectives and are not duplicative:

- Director of Federal Grant Initiatives;
- Grants Unit Representative; and
- Strategic Planning Section Commanding Officer or designee.

Request Process

Position	Process
Employees	• Shall Notify the Director of Federal Grant Initiatives of intent to apply for a grant as soon as feasible, before the SP 426 deadline. • Shall submit all requests through channels to the appropriate Division Commander or designee, **at least fifteen (15) days prior to the filing date deadline**; • Submitted requests shall include the following information; o A completed SP 426; o A copy of the original solicitation/application that identifies the funding source and requirements i.e. eligibility, application deadline, and matching amount requirements; o A program statement narrative that identifies the goals and objectives, as well as the intended outcome to be accomplished, and any supporting documentation; and o A budget which includes current information regarding personnel and/or equipment costs andthe services to be performed and/or purchased.
Division Commander or Designee	• Shall review all requests; • Ensure adequate time is available to allow for modifications to the application before the filing deadline; • Endorse the SP 426; • Forward the request to the Strategic Planning Section; and • Designate a Project Administrator.
Director of Federal Grant Initiatives	• Shall review the request with the designated Project Administrator; • Notify the fiscal Grants Unit; • Ensure the application adheres to program guidelines and includes all required information and attachments; and • Shall document grant requests and maintain electronic copies of grant requests and SP-426 forms.
Grants Unit	• Ensure the request budget is appropriate and accurate; and • Assist as needed with questions pertaining to budget and finance.

Request Process, continued

Strategic Planning Section Commander	• Shall immediately review the request to ensure it aligns with Departmental goals and objectives; • Confirm that the request has been reviewed by the Director of Federal Grant Initiatives and Grants Unit; • Forward completed requests to the Chief Administrative Officer and the Colonel/Superintendent for approval; and • Maintain hard copies of completed applications and SP-426 forms.
Colonel/ Superintendent	• Approve or deny the request; • If approved, sign the original application and the SP426.

References: ADM-30 Asset Management;
SP 426 Grant/Agreement Approval Request Form.

Promulgated By:

Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**ADM-09**
Subject:	
Line Inspection	

Policy

Line Inspections shall be conducted to improve the operational readiness of the Department by ensuring that all members adhere to all established rules, regulations, policies, procedures, orders, directives, and general laws.

Members shall immediately correct unsatisfactory behavior and conditions in order to avoid the consequences which erode the trust and confidence of the public.

Procedure

Members from the rank of Captain through Trooper shall be inspected.

Members assigned to duties requiring civilian attire are exempt from the uniform/appearance portion of the inspection.

Troop/Section Commanders may require additional line inspection procedures within their respective commands.

Line Inspections

Troop/Section Commanders or designee, shall:

- Oversee the entire line inspection program for their command;
- Ensure that all members are inspected at least quarterly by their first line supervisor; and
- Ensure inspections are properly documented on PayStation.

First Line Supervisors Duties

First Line Supervisors shall:

- Conduct an inspection of all immediate subordinates at least quarterly, including their assigned cruisers and equipment; and
- Submit a report of the inspection, including an explanation of the inadequacies, via PayStation, quarterly during the months of January, April, July, and October.

Minor deficiencies which can be corrected during the course of a first line inspection, may be reported as adequate via PayStation. Repeated minor deficiencies shall be documented on an Employee Evaluation System (EES) form.

First Line Supervisors Duties, continued

Use Line Inspections shall include:

- Personnel: Uniform, equipment, appearance, cleanliness/neatness, jewelry, hygiene, cosmetics, and hair;
- Use of force equipment: All issued use of force equipment;
- Cruiser: General condition, issued equipment, cleanliness, and maintenance;
- Citations and audit sheets: Review citations and audit sheets, ensure documentation for racial profiling requirements are correctly submitted; and
- Licenses and Identification Cards e.g., Massachusetts Driver's License, License to Carry Firearms, and Department Identification Cards.

Reviewing Supervisor Duties

Each submitted inspection report shall be reviewed by a second level supervisor prior to approval via PayStation. The reviewing supervisor shall:

- Discuss any deficiencies noted within the report with the inspecting member prior to approving the report; and
- Take corrective action to ensure that all deficiencies and inadequacies are addressed.

Station/Unit Inspection

Station/Unit inspections shall be performed in conjunction with the Annual Fixed Assets Inventory. Station/Unit Commanders shall examine Department facilities and determine where there are inadequacies, deficiencies or areas not otherwise in compliance with Department rules, regulations, policies, procedures, orders, directives, and general laws.

Any written reports generated shall be forwarded to the Troop Commander through channels.

Annual inspections shall include at a minimum:

- Buildings and grounds of facility: Conduct a general inspection of the facility with attention to the condition of maintenance and safety issues;
- Entrances, exits, and security;
- Public accommodation: Parking, handicap access, toilet facilities/ public restrooms, and lobby area;
- Holding facilities: As required under DET-04 Holding Facilities; and
- Employee cards/records: Are current and complete for all assigned employees.

Subject:	Number:
Line Inspection	**ADM-09**

References: ADM-30 Asset Management;
DET-04 Holding Facilities.

Promulgated By:

Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**ADM-09A**
Subject:	
Staff Inspections	

Policy

The Department shall continuously audit and inspect all resources, facilities, equipment, personnel, practices and policies, to update the Command Staff on the quality of Department services.

Staff Inspections Protocols

To accomplish the mission of conducting Staff Inspections, inspectors shall have complete and unrestricted access to all Department records and properties.

Office of Professional Integrity and Accountability (OPIA) shall:

- Conduct Staff Inspections on all resources, entities, and facilities within the Department;
- Conduct open inspections with the full knowledge and cooperation of everyone involved;
- Notify the appropriate Commanders of the intended date and scope any inspections at least seven (7) days in advance of the inspection; and
- Include a list of those materials, files, and subjects to be reviewed or examined by the inspector.

Troop/Section Commanders shall work cooperatively with the inspector, and shall prepare and provide all materials requested.

Upon request of the appropriate Division Commander, inspectors may conduct unannounced inspections of any Department entity.

Routine Staff Inspections

Routine Staff Inspections may include:

- Narcotics, contraband and physical evidence;
- Seized monies/asset forfeiture;
- Payroll entries, including overtime and details;
- Automated Vehicle Locator Technology (AVL);
- Body-Worn and Cruiser-Mounted Camera footage;
- Detail inspections;
- Found/held property;

Routine Staff Inspections, continued

- Holding facilities;
- Racial profiling compliance;
- Line inspections;
- Administrative journals and records;
- Issued Department equipment; and
- Other areas as directed by the Division Commander of Standards and Training.

Inspection Finding and Reports

Inspectors shall prepare and submit a detailed report through appropriate channels to the Colonel/Superintendent within sixty (60) days of each inspection.
This report shall include, at a minimum:

- Findings and observations; and
- Opinions, recommendations and conclusions.

Copies of this report shall also be forwarded to the appropriate Division Commander.

Upon receipt of a Staff Inspection Report, Troop/Section Commanders shall submit a report outlining the specific actions taken to ensure correction of all deficiencies noted. This report shall be submitted within thirty (30) days to the appropriate Division Commander, with a copy to be forwarded to the Division Commander of Standards and Training.

References: ADM-19B Automatic Vehicle Locator (AVL) Technology;
ADM-35 Body-Worn and Cruiser-Mounted Cameras;
MPAC: 84.1.6.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**ADM-10**
Subject:	
Awards	

Policy

The Department shall make every effort to recognize the people whose actions assist the Department in carrying out its mission and who go beyond normal expectations or requirements.

EES Coordinator

The Employee Evaluation System (EES) Coordinator shall be a Commissioned Officer or Program Coordinator designated by the Division Commander of Standards and Training or designee. The EES Coordinator shall be responsible for the Awards Board's administrative duties, preservation of all records, and shall not be a voting member of the Awards Board.

Standard Operating Procedure

The EES Coordinator shall develop a standard operating procedure that details:

- The Board's organization and procedures; and
- Board member duties and responsibilities.

Awards

State Police Members	
Medal of Honor Gold Medal Blue/Yellow/Blue Ribbon	Established to honor Department members who have performed acts of extraordinary heroism above and beyond the call of duty. <u>Elements of consideration are:</u> • Actions that depict outstanding bravery, courage, and self-sacrifice, or overriding concern for others; • Heroic actions taken for the rescue of life or in defense of another life; • Actions taken notwithstanding the potential of being killed; or • Valorous sacrifice (severe injury or loss of life).

Awards, continued

Sworn Police Officers	
Medal of Valor Silver Medal White/Red/Blue/Red/White Ribbon	Established to bestow recognition upon police officers who have performed specific acts of bravery or have exhibited outstanding courage while performing their duties. Elements of consideration are: • An act characterized by courage, daring, and bravery; • The officer took immediate and decisive action to avert injury or loss of life to others; • While in a hazardous environment, the officer exhibited outstanding courage while performing their duties; • The officer rescued or defended another; or • Valorous sacrifice (severe injury or loss of life).
Medal of Merit Bronze Medal Blue/White Ribbon	Established to bestow recognition upon police officers who have performed acts of outstanding achievement, far exceeding normal demands of the Department, which greatly contribute to the operation of the Department. Elements of consideration are: • Noteworthy achievements that greatly contributed to a Department operation or a community; • An exemplary act characterized by ingenuity, devotion, creativity, boldness, and outstanding professional conduct; or • Action(s) that reflects great credit to the member and the Department.
Medal of Lifesaving Bronze Medal Red/White Ribbon	Established to bestow recognition upon police officers who undertake significant actions in the saving of another life. Elements of consideration are: • Actions were taken for the preservation of another life; and • The actions actually preserved life. Note: Documentation should be submitted supporting the life threatening nature of the injuries or circumstances.

Awards, continued

Sworn Police Officers and Members of the Public

Superintendent's Commendation Plaque	Established to bestow recognition upon an employee of the Department, or a member of the public, who has made an exceptional contribution to the Department. Elements of consideration are: • Extraordinary performance that clearly distinguishes the individual; • Performance that significantly contributes to Department operations; • Actions that significantly enhance the positive image of the Department; • Exceptional contribution(s) to the Department; or • Exceptional service to the community.
Division Commander's Commendation Certificate	Established to bestow recognition upon an employee of the Department, or a member of the public, who has made a significant contribution to a Division. Elements of consideration are: • Notable performance that clearly distinguishes the individual; • Performance that notably contributes to the Division's operations; • Actions that notably enhance the positive image of a Division; • Exceptional contribution(s) to a Division; or • Exceptional service to the community.
Troop/Section Commander's Commendation Certificate	Established to bestow recognition upon an employee of the Department, or a member of the public, who has made a significant contribution to their Station/Section/Unit, or, upon a member of the public who has made a significant contribution to any Station/Section/Unit, or the Department. Elements of consideration are: • Notable performance that clearly distinguishes the individual, • Exceptional contribution(s) to the Station/Section/Unit; or • Exceptional service to the community.

Awards, continued

Department Entities

Superintendent's Unit Citation Plaque	Established to bestow recognition upon the employees of a particular Station/Section/Unit who have made an exceptional contribution to the Department. Elements of consideration are: • Extraordinary performance that clearly distinguishes the Station/Section/Unit; • The successful conclusion or culmination of a significant investigation or achievement of a significant project; • The achievement of outstanding enforcement efforts by a Station/Section/Unit; • Superior support efforts to the Department; or • Actions that significantly increase the positive image of the Department.

Civilians

Distinguished Service Award Gold Medal Red/White/Blue Ribbon	Established as the highest award to bestow recognition upon an employee of the Department, or a member of the public, who has provided extraordinary assistance to the Department. Elements of consideration are: • Heroic actions were taken for the rescue of life, or in defense of an officer or other person; • The individual, while assisting the Department, imperilled himself/herself to the risk of great personal injury, or death; • The individual aided an officer in a critical situation and in need of help; or • The individual's extraordinary actions/achievements greatly contributed to a significant Department operation.

Awards, continued

Civilians	
Lifesaving Award Red/White Lapel Pin	Established to bestow recognition upon an employee of the Department, or member of the public, who undertakes significant actions in the saving of another life. Elements of consideration are: • Actions were taken for the preservation of another life; and • The actions preserved life. Note: Documentation should be submitted supporting the life threatening nature of the injuries or circumstances.
Public Service Award Certificate	Established to recognize an employee of the Department, or a member of the public, who has provided outstanding assistance to the Department, or has significantly contributed to public safety. Elements of consideration are: • Significant actions contributing to Department objectives; • Significant actions contributing to the betterment of policing or public safety; • Noteworthy achievements that greatly contributed to a Department operation; or • Noteworthy achievements that greatly contributed to a community.

Nomination Procedure

Step	Action
1	Supervisors shall make nominations according to the following process: **Department Members** • Consult the list of the Awards Board criteria; • Complete an electronic EES Supervisory Observation Report or an EES quarterly performance evaluation; and • Electronically forward, through channels, within the awards database designated by the Division of Standards & Training, the respective award recommendation and reasoning (i.e. Medal of Valor) to the appropriate Division Commander. • Attach any supporting documentation relevant to the submission within the awards database. **Department Civilian Employees or Non-Department Individuals** Nominations for awards to civilian employees or non-department individuals shall be forwarded to the Awards Board as outlined above.

Nomination Procedure, continued

2	Division Commanders shall: • Determine if the act is worthy of recognition; • Electronically forward, within the awards database, the respective award recommendation(s) to the EES Coordinator and the Awards Board. • Ensure all documentation supporting the award selection is electronically attached/uploaded within the awards database.
3	The Awards Board shall: • Meet biannually (twice a year) or as needed to review recommendations from the Division Commanders; • Make recommendations to the Colonel/Superintendent based upon a majority vote; and • Return recommendations, which do not rise to the level of an award, to the appropriate the Division Commander.
4	The Colonel/Superintendent shall: • Review the biannual recommendations from the Awards Board; and • Notify the Awards Board of any changes to the recommendations.

Non-Department Nominations

Nominations for awards given by organizations outside the Department shall be forwarded to the Awards Board as outlined above.

Ceremony Procedures

Awards shall be presented at least biannually, at ceremonies scheduled during the months of April and October. The Colonel/Superintendent may hold additional ceremonies as deemed necessary.

Position	Duties
Awards Board	• Notify each Division Commander, in writing of all actions taken regarding the awards nominations for that Division; and • Notify Media Relations of the nominees at least forty-five (45) days before the next scheduled ceremony.
Media Relations	• Arrange for award ceremonies in April and October of each year; and • Ensure the award recipients have been notified, through the Office of the Superintendent, in writing at least thirty (30) days before the ceremony.

Ceremony Procedures, continued

Position	Duties
Human Resources	• Maintain a database containing all of the awards recipients' specifics; and • Place supporting award files in recipients' Personnel Files.
Office of the Superintendent	• Notify Award recipients of their invitation to the Awards ceremony at least thirty (30) days before the ceremony.
Colonel/ Superintendent	• Present the awards.
Division Commander	• Generate and print Division Commander Commendation Certificates and Troop/Section Commendation Certificates; • Present Division Commander Commendation Certificates to the recipient in hand; and • Electronically record the issuance of the award.
Troop/Section Commander	• Present Troop/Section Commendation Certificates to the recipient in hand; and • Electronically record the issuance of the award.

Awards Board Composition

The Awards Board shall be comprised of nine (9) employees with eight (8) voting members. Awards shall be approved based on a majority vote. Employees shall serve for a minimum term of one (1) year.

Representative	Rank/Position	Designated by:
President	Major	Superintendent
Department Employee	Civilian	Deputy Superintendent
Field Services	Captain or lower	Division Commander
Investigative Services	Captain or lower	Division Commander
Standards and Training	Captain or lower	Division Commander
Administrative Services	Captain or lower	Division Commander
Homeland Security and Preparedness	Captain or lower	Division Commander
Forensic Services	Captain or lower	Division Commander
EES Coordinator	Commissioned Officer/Program Coordinator Non-Voting Member	Division Commander of Standards and Training

Other Awards

Supervisors may establish:

- Other forms of recognition as necessary and electronically document the issuance of any recognition in the EES system. These recognitions shall not be deemed to be a Department Award within the guidelines of this policy.

Exceptions

In extraordinary circumstances the Awards Board may:

- Vote to make an exception to this policy, providing the vote is unanimous; and
- Forward the exception to the Colonel/Superintendent for approval.

References: Department Employee Evaluation System (EES);
MPAC: 26.1.2.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**ADM-11**
Subject:	
Sick Leave	

Policy

The Department recognizes the importance of Sick Leave for its sworn members and their families.

The Department has a responsibility to monitor the use of Sick Leave to prevent abuses.

For the purposes of this policy, the term member(s) shall refer to sworn Department members.

Sick Leave Credits

Sick Leave credits are granted in accordance with provisions of the applicable Collective Bargaining Agreement (CBA) and the Department's Rules and Regulations. The Collective Bargaining Agreement also provides guidelines for the administration of Sick Leave.

Granting Sick Leave

Sick Leave is granted at the discretion of the Colonel/Superintendent, or designee, to a sworn member when the member cannot perform their duties because they are incapacitated by:

- Personal illness or injury;
- The presence of the member at their work location would jeopardize the health of others through exposure to a contagious condition; or
- The member's spouse, child, parent, or spouse's parent, or relative living in the member's household, is seriously ill. In this event, a limit to the amount of leave the member can use is set by the CBA and federal and state laws.

Notifying duty assignment of intention to use Sick Leave

As early as possible on the first day of a Sick Leave absence, a member shall notify their duty assignment of the intention to use Sick Leave. The member shall notify their duty assignment of the anticipated duration of the Sick Leave absence. If the absence is shorter than, or extends beyond, the initially anticipated period of absence, the member shall advise their duty assignment of the modification to the Sick Leave request. The Sick Leave request shall be appropriately logged in the Department's time and attendance system and in the Daily Administrative Journal and shall only reflect the member's name, identification number, and type of Sick Leave.

Subject:	Number:
Sick Leave	**ADM-11**

Notifying duty assignment of intention to use Sick Leave, continued

Supervisors shall be informed of:

- The nature of the illness or injury, and anticipated duration of absence, if known;
- The location of their recuperation and a telephone number; and
- Any duties or scheduled court appearances that may require attention.

If using Sick Leave in excess of five (5) consecutive work days, the member may be required to undergo a medical examination, or provide documentation from a licensed medical practitioner, to determine their fitness for duty.

Sick Leave

Members who are granted Sick Leave shall not request or work overtime and/or details within twenty-four (24) hours from the start time of their regularly scheduled work shift, unless the members has:

- Worked at least four (4) or more consecutive hours during the first half of their shift for which Sick Leave was granted; or
- Worked at least four (4) or more consecutive hours during the second half of their shift for which Sick Leave was granted.

Members may utilize Sick Leave to attend doctor and dental appointments.

Note: Supervisors shall ensure compliance with ADM-19 Vehicle Management with regards to Department issued vehicles.

Cancelling Sick Leave

If a member is returning to work earlier than previously reported, the member shall call to cancel the remaining Sick Leave at least eight (8) hours prior to the reporting start time of their next shift.

Location of Recuperation

Members using Sick Leave may leave the Commonwealth of Massachusetts only:

- With authorization of their Commanding Officer; and
- To obtain medical care as prescribed by their licensed medical practitioner.

Members utilizing Sick Leave may be ordered to remain at a reported place of recuperation. A reasonable time period away from this location is allowed to:

- Obtain services or products consistent with medical care;
- Vote or attend religious services;
- Attend to an emergency situation; or
- Attend to other matters with the permission of their supervisor.

Subject:	Number:
Sick Leave	**ADM-11**

Review of Sick Leave

Supervisors at all levels are responsible for monitoring Sick Leave. Supervisors should review attendance records for signs of Sick Leave abuse, preferably in conjunction with the Employee Evaluation System (EES).

Some potential signs of Sick Leave abuse are:

- Excessive use;
- Patterns of use, such as before or after days off, or on weekends;
- Use on or around a holiday;
- Use after working overtime, details, or extra shifts;
- Use when the member has indicated that they want time off;
- Use when the supervisor believes that the member is not sick; and
- When the Sick Leave repeatedly creates shortages or overtime.

When a supervisor has *reason to suspect* Sick Leave abuse, the supervisor has the following options:

- Reason to Suspect Abuse in General- Notify the member using the SP 382 Abuse of Sick Leave form. This advises the member that future Sick Leave may be subject to extra scrutiny; or
- Reason to Suspect Abuse in a Particular Instance- Notify the member using the SP 383 Submission of Medical Evidence form. The member is then required to produce satisfactory medical evidence by submitting the SP 384 Request for Certification of Medical Condition form within seven (7) days.

Supervisors should have articulable reasons for suspecting abuse before filing the SP 382 Abuse of Sick Leave form. Supervisors may call or visit the member at their place of recuperation to verify the use of Sick Leave. Calls or visits shall not occur between 2200 hours and 0800 hours.

Members who abuse Sick Leave or who are excessively absent from duty may be subject to administrative or disciplinary action and denial of Sick Leave.

Leave Benefits

Leave issues for members are addressed in the Collective Bargaining Agreement.

Commanding Officers shall consult applicable collective bargaining agreements for civilians under their charge.

Subject:	Number:
Sick Leave	**ADM-11**

References: ADM-19 Vehicle Management;
ADM-25 Paid Details;
SP 382 Abuse of Sick Leave;
SP 383 Submission of Medical Evidence;
SP 384 Request for Certification of Medical Condition;
State Police Association of Massachusetts Collective Bargaining Agreement.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**ADM-11A**
Subject:	
Temporary Modified Duty	

Policy

Temporary Modified Duty provides an alternative work assignment for eligible members who are temporarily unable to meet some Department in-service standards. Members failing to meet in-service medical and physical fitness standards due to temporary injury, illness or incapacitation are eligible to undergo re-examination pursuant to M.G.L. c. 22C, §10. Requests for re-examinations shall be made in writing to the Colonel/Superintendent within the period prescribed by M.G.L. c. 22C, §10 or shall be waived.

Temporary Modified Duty

While on Temporary Modified Duty, members shall not:

- Wear a uniform;
- Work overtime;
- Work paid details; and
- Have contact with prisoners, the public in an enforcement capacity, or function as a desk officer in a sub-station.
  Exception: Emergency situations may require the immediate response of the member.

The Colonel/Superintendent may authorize members on Temporary Modified Duty to:

- Operate a Department vehicle; and/or
- Carry a Department issued firearm.

The immediate supervisor of a member on Temporary Modified Duty shall ensure compliance with ADM-19 Vehicle Management.

Eligibility

Eligibility for Temporary Modified Duty status shall:

1. Be recommended by the State Police Surgeon;
2. Require that the member's anticipated period of injury, illness or incapacitation be temporary in nature, meaning less than twelve (12) months in duration; and
3. Be determined by the Colonel/Superintendent.

Members who are not eligible for Temporary Modified Duty may:

- Remain or be placed on Sick Leave, Injured Leave, or other approved duty or leave status as appropriate.

Evaluation by State Police Surgeon

Members who are eligible or assigned to Temporary Modified Duty shall be required to:

- Submit to periodic medical evaluation(s) of their condition as determined by the State Police Surgeon or by order of the Colonel/Superintendent.

Any member who has been assigned to Temporary Modified Duty for a period of twelve (12) months, shall be examined by the State Police Surgeon, who, after reviewing all medical information, shall recommend to the Colonel/Superintendent that the member:

- Remain on Temporary Modified Duty for a period as recommended by the State Police Surgeon and as determined by the Colonel/Superintendent;
- Submit to a medical examination as directed by the Department;
- Be placed on: Full Duty; No Duty; or Temporary Modified Duty; and/or
- Be discharged, separated and/or the member may retire.

Member's Assignment to Temporary Modified Duty

The Colonel/Superintendent may assign a member to Temporary Modified Duty based upon a medical recommendation from the State Police Surgeon. A member may dispute such assignment by:

- Providing a written notification to the Colonel/Superintendent within ten (10) days; and
- Producing a written statement from the member's physician detailing the medical reasons the member cannot perform such assignment.

The Colonel/Superintendent upon receipt of such written notification may:

- Require the member to submit to an examination by a medical physician selected by the Department.

The medical physician selected by the Department shall:

- Examine the member to determine if the member can perform the duties of the proposed assignment; and
- Forward written documentation of the examination with recommendations to the Colonel/Superintendent.

The Colonel/Superintendent shall make all final determinations regarding a member's assignment to Temporary Modified Duty.

Responsibilities

Position	Duties
Colonel/Superintendent	Shall establish and approve Departmental: • Duty Status; • Leave Status; • Medical Standards; and • In-service Standards.
State Police Surgeon	Shall evaluate members and recommend: • Eligibility for Temporary Modified Duty status; and • The frequency of medical evaluation periods.

Return to Duty

Any leave or break in service 90 days – 1 year:

Members returning from any leave, temporary modified duty or break in service exceeding ninety (90) days requesting full duty status shall ensure the tasks below are completed in the following sequence:

- The members' Station / Section / Unit Commander shall notify Human Resources in advance of date of return and request the member is returned to full duty;
- Human Resources will notify the Division of Standards and Training Commander or designee when the member is returned to full duty;
- The member shall then be required to successfully complete:
    - Online academy;
    - Refresher training in the following areas (if deemed necessary by the Division of Standards and Training Commander or designee):
        1. Patrol Procedures
        2. Defensive Tactics
        3. EVOC
        4. Firearms (reissuance of assigned UOF gear and requalification if necessary)
- Upon satisfactory completion of training, the Station / Section / Unit Commanders will be advised by the Commandant of the State Police Academy.

Any leave or break in service exceeding 1 year:

Members returning from any leave or break in service exceeding one (1) year requesting full duty status shall ensure the tasks below are completed in the following sequence:

- The members' Station / Section / Unit Commander shall notify Human Resources in advance of date of return and request the member is returned to full duty.

Return to Duty, continued

- The member shall then be required to successfully complete:
  - A background investigation;
  - A medical examination by the State Police Surgeon to include drug testing; and
  - Psychological testing.

Human Resources will notify the Division of Standards and Training Commander or designee when the member is returned to full duty.

The member shall then be required to successfully complete:

- Online academy
- Refresher training in the following areas (if deemed necessary by the Division of Standards and Training Commander or designee):
  - Patrol Procedures
  - Defensive Tactics
  - EVOC
  - Firearms (reissuance of assigned UOF gear and requalification if necessary)
- Upon satisfactory completion of training, the Station / Section / Unit Commanders will be advised by the Commandant of the State Police Academy.

Former members wishing to return from a separation from service that exceeds three (3) years shall:

- Meet all requirements for re-entry to the Department; and
- Successfully complete the Recruit Training for appointment to the position of Trooper.

Note: Failure to successfully complete the Recruit Training may affect pension benefits, if applicable.

References: ADM-19 Vehicle Management;
MGL c.22C, § 10.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**ADM-11B**
Subject:	
Injury Reporting and Leave	

Policy

The Department shall investigate and document each on-duty injury sustained by a member. All duty related injury documentation shall be completed and forwarded to the proper authority in a timely manner.

Every injury shall be investigated in accordance with this policy.

Leave Status

Members incapacitated by an injury incurred on-duty shall:

- Be placed on *Injured Leave Pending* (ILP) status by their Commanding Officer or designee until examined by the State Police Surgeon; and
- Officially be placed on *Injured Leave Duty* (ILD) status when so determined and approved by the Board on Claims.

Payroll Information

A member who:

- Remains on approved ILD into the next calendar year, or
- Returns from approved ILD in the last quarter of the current calendar year may request:
  - The Colonel/Superintendent to convert excess vacation time credits to sick leave.

Members on approved ILD may request a tax exempt status letter through the Payroll Section.

Reporting

If injured while on-duty:

- Division of Field Services members shall immediately advise the Desk Officer who shall notify the Troop Duty Officer; and
- Non-Field Services members shall notify their Commanding Officer.

The nature and cause(s) of a member's injury shall be noted in the Daily Administrative Journal.

Supervisors shall ensure the procedures outlined in TRF-20 Department Vehicle Crashes are followed, if an injury is the result of a cruiser crash.

Investigation/ Documentation Protocols

The **Troop Duty Officer** (for DFS members) or the **Commanding Officer** (for non-DFS member) shall:

- Assign an investigating officer;
- Ensure that form SP 624 Initial Injury Report is completed; and
- Ensure that prior to the end of the shift, the SP 624 is sent via fax or email to General Headquarters Division Commander and the Occupational Health Unit/Human Resources Section.

Injured members should, if necessary, seek emergency medical care or seek treatment from their own personal physician. All bills shall be:

- Made out in the injured member's name and home address;
- Itemized and initialled by the member; and
- Submitted to the investigating officer within seven (7) days.

Injured members (unless physically incapable) shall, within seven (7) days, complete and sign the following forms and submit to the investigating officer:
Sections 1 through 7 of SP 37 Statement in Support of Claim;

- Commonwealth's Form 1 Notice of Injury;
- To/From Letter (including how the injury occurred and names of any witnesses and statements); and
- Authorization for Release of Medical Records.

Investigating officers shall:
When the injured members are physically incapable:

- Prepare the appropriate forms (e.g. SP 37); and
- Forward same on the injured member's behalf.

Within seven (7) days of receipt of claim, submit to the Troop/Section/Unit Commander:

- Statement in Support of Claim, after completing Section 8;
- Notice of Injury;
- Injured member's To-From along with all supporting documentation;
- Any witness statements; and
- Medical Records and Medical Bills, as available.

Troop/Section/Unit Commander shall:

- Complete Section 9 of the Statement in Support of Claim;
- Prepare a To/From letter to the President of the Board on Claims, which shall include a brief account of the facts concerning the injury and conclusions regarding the cause of the injury and forward:
    - Investigating Officer's Report and documentation; and
    - The Statement in Support of Claims.
- Forward a copy of the Board on Claims decision letter to the injured member.

Investigation/ Documentation Protocols, continued

Troop/Section/Unit Commanding Officer shall, if the injured member is unable to return to duty:

- Place the member on ILP (members who have a recurrence of a previous injury should be placed on Sick Leave); and
- Notify the Occupational Health Unit of the status and request an appointment with the State Police Surgeon.

The **State Police Surgeon** shall:

- Conduct an initial evaluation of the injured member to determine the member's duty status;
- Schedule periodical examinations as deemed necessary to determine the member's duty status;
- Determine and recommend a member's eligibility for Modified Duty; and
- Report to the Department when a member is medically able to return to full duty status.

Recurrent Injuries

All recurrent injuries shall be reported using the same process as new injuries.

Members with any recurrent injuries shall be placed on Sick Leave until officially approved and placed on ILD status.

While on Injured Leave

Members on injured leave may only leave the Commonwealth:

- With authorization of their Commanding Officer.

Supervisors shall ensure compliance with:

- ADM-19 Vehicle Management with regards to Department issued vehicles; and
- ADM-20 Weapons Management with regards to Department issued weapons.

Return to Duty

<u>Any leave or break in service 90 days – 1 year:</u>

Members returning from <u>any</u> leave, temporary modified duty or break in service exceeding ninety (90) days requesting full duty status shall ensure the tasks below are completed in the following sequence:

- The members' Station / Section / Unit Commander shall notify Human Resources in advance of date of return and request the member is returned to full duty;
- Human Resources will notify the Division of Standards and Training Commander or designee when the member is returned to full duty;

Return to Duty, continued

- The member shall then be required to successfully complete:
  - Online academy;
  - Refresher training in the following areas (if deemed necessary by the Division of Standards and Training Commander or designee):
    1. Patrol Procedures
    2. Defensive Tactics
    3. EVOC
    4. Firearms (reissuance of assigned UOF gear and requalification if necessary)
- Upon satisfactory completion of training, the Station / Section / Unit Commanders will be advised by the Commandant of the State Police Academy.

Any leave or break in service exceeding 1 year:

Members returning from any leave or break in service exceeding one (1) year requesting full duty status shall ensure the tasks below are completed in the following sequence:

- The members' Station / Section / Unit Commander shall notify Human Resources in advance of date of return and request the member is returned to full duty.
- The member shall then be required to successfully complete:
  - A background investigation;
  - A medical examination by the State Police Surgeon to include drug testing; and
  - Psychological testing.

Human Resources will notify the Division of Standards and Training Commander or designee when the member is returned to full duty.

The member shall then be required to successfully complete:

- Online academy
- Refresher training in the following areas (if deemed necessary by the Division of Standards and Training Commander or designee):
  - Patrol Procedures
  - Defensive Tactics
  - EVOC
  - Firearms (reissuance of assigned UOF gear and requalification if necessary)
- Upon satisfactory completion of training, the Station / Section / Unit Commanders will be advised by the Commandant of the State Police Academy.

Former members wishing to return from a separation from service that exceeds three (3) years shall:

- Meet all requirements for re-entry to the Department; and
- Successfully complete the Recruit Training for appointment to the position of Trooper.

Note: Failure to successfully complete the Recruit Training may affect pension benefits, if applicable.

References: SP 37 Statement in Support of Claim Form;
SP 624 Initial Injury Report;
Commonwealth's Form 1 Notice of Injury;
TRF-20 Department Vehicle Crashes;
ADM-19 Vehicle Management;
ADM-20 Weapons Management;
Rules and Regulations Article 8.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

1647

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**ADM-11C**

Subject:

Maternity Leave and Guidelines

Policy

The maternity policy is designed to provide notification and employment guidelines in order to prevent workplace discrimination based on pregnancy.

Members shall:
- Not be required to disclose her pregnancy except in accordance with this policy.

The Department shall only take action when;
- Requested by the member; or
- The member's physician or obstetrician recommends work limitations.

Notification Requirements

A member shall notify her commanding officer that she is pregnant, when she has:
- Reached her third trimester of pregnancy;
- Requested modification, exemption, or leave from her assigned duties; or
- Been given physical restrictions or limitations by her healthcare provider that prohibits her from performing all aspects of her current assignment.

All notifications shall be made:
- In writing, and include the anticipated due date as well as the anticipated date of return to work (if known).

Notification Process

The member shall submit to her commanding officer:
- Within seven (7) days of the initial notification, a letter from her healthcare provider regarding her pregnancy; and
- Every thirty (30) days thereafter, a written update from her attending physician or obstetrician.

Notification Process, continued

Each letter shall contain:

- Name, address and contact information for the attending healthcare provider;
- Any restriction or limitation on her current work assignment, if none, the letter shall explicitly state so;
- Anticipated due date;
- Anticipated date for return to work (if known); and
- Any other information the member or healthcare provider believes would be of assistance to the Department.

Duty Status

A member not placed on alternative duty shall:

- Perform all duties required of her in her current position until such time as other duties are assigned consistent with this policy.

If the member has not notified the Department of her pregnancy and sought alternative duty status under this policy then her pregnancy:

- Cannot be a defense to any disciplinary action taken against her for failure to perform her duties.

A member may request in writing, at any time during her pregnancy, to be assigned to alternative duty. Alternative duty shall:

- Not affect the member's existing benefits;
- Be consistent with restrictions or limitations identified by her attending regarding:
  - Overtime and paid details;
  - Interaction with prisoners;
  - Interactions with the public in an enforcement capacity; and
  - Dangerous duty such as riots.

  <u>Exception</u>: Any emergency situation that may require the immediate response of the member.

Voluntary Alternative Duty

The Colonel/Superintendent or designee shall:

- Approve and determine a member's request for alternative duty assignment taking into consideration the pregnant member's current assignment and duties.

Eligibility for an alternative duty assignment:

- Does not entitle the member to be transferred to a different position or unit within the Department.

Alternative duty may be:

- A form of modified duties and/or an altered work shift at the request of the member; and
- Consistent with any restrictions or limitations set forth by her attending healthcare provider.

Voluntary Alternative Duty, continued

Eligible Members:

- Shall not be transferred or have their shift changed involuntarily as the result of seeking alternative duty, however, a reasonable accommodation may require the member to accept temporary assignment in the geographic area of her current assignment or residence.

Involuntary Alternative Duty

The Department may involuntarily reassign a member to alternative duty based upon medical evidence that the member cannot safely perform her current duties.

A member may challenge such reassignment by:

- Providing a statement from her healthcare provider that she can perform such duties;
- Submit to an examination by a neutral healthcare provider selected by the member from a list agreed upon by the Department and the representatives of the member's collective bargaining unit;
- Remain in her current duty assignment pending receipt of the opinion of the neutral healthcare provider; and
- Be bound by the opinion of the neutral healthcare provider.

The neutral healthcare provider shall:

- Examine the member and determine whether she can perform the duties of her assigned position; and
- Render an opinion which shall be binding upon the Department and the member.

Duty Assignment

When an alternative duty assignment is unavailable within a member's current assignment, the Colonel/Superintendent or designee shall:

- Find an appropriate alternative assignment within the member's immediate geographic area as defined by the Troop Area of her current assignment or her residence; and
- Ensure no member be denied such an assignment within her current assignment or immediate geographic area.

If a member believes that she has been unreasonably denied such an assignment in violation of this policy the member shall:

- Submit a To-From outlining the objections to the Colonel/Superintendent or designee.

The Colonel/Superintendent or designee shall:

- Endeavor to remedy the member's concerns within seventy-two (72) hours of receipt of the notice; or
- Respond, in writing, stating the position of the Department with respect to the request.

Department Standards

A member who has notified the Department of her pregnancy in accordance with this policy shall:

- Be exempt from weapons qualification requirements during the course of her pregnancy; and
- Be required, upon return to full duty status, to meet the Department's medical and in-service standards.

Department Issued Vehicles

A member who is placed on alternative duty shall be:

- Issued an unmarked vehicle while on an alternative duty status.

If the Department is unable to provide the member with an unmarked vehicle, the member shall be:

- Provided with a per diem rate in accordance with the same terms and conditions as apply to members of equal rank assigned to the Massachusetts Port Authority.

Members who are currently assigned an unmarked vehicle shall be allowed to continue to operate the vehicle.

Supervisors shall ensure compliance with:

- ADM-19 Vehicle Management with regards to Department issued vehicles.

Members Rights

The member retains all such rights available to her under the collective bargaining agreement, state and federal law to challenge the decision of the Colonel/Superintendent or designee with respect to such a determination by the Colonel/Superintendent or designee as to the implementation of this policy.

References: ADM-19 Vehicle Management;
MPAC: 22.2.0.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**ADM-11E**
Subject:	
Leaves of Absence	

Policy

The Department may grant to a sworn or a civilian employee a leave of absence, with or without pay, as allowed by:

- Federal and state law;
- Commonwealth's Human Resources Division (HRD);
- Collective Bargaining Agreements (CBA), Personnel Administration Rules (PAR), HRD Red Book;
- Military Leave pursuant to ADM-26 Military Service; or
- The Colonel/Superintendent.

Leave Coordinator

The Division of Administrative Services (DAS) Commander shall appoint a Leave Coordinator who shall be responsible for:

- Receiving and processing specified requests for leave;
- Assisting employees with paperwork requirements;
- Assisting and coordinating with Commanding Officers and the Colonel/Superintendent to evaluate requests for leave;
- Coordinating the requirements for employees returning from leave;
- Ensuring personnel records, payroll history, health insurance and other benefits are updated or administered as necessary; and
- Consulting with Office of Employee Relations and Legal Section regarding leave requests.

Approval of Leave

The Leave Coordinator shall forward all requests for leave to the Colonel/Superintendent. The Colonel/Superintendent may approve or deny leave based upon:

- Applicable federal and state laws, and collective bargaining agreements;
- Operational needs of the Department;
- The purpose of the leave; and/or
- Other factors that may exist.

The Leave Coordinator shall notify an employee, in writing, of the decision of the Colonel/Superintendent.

Conduct on Leave

An employee on a leave of absence for any duration shall:

- Adhere to and abide by all Department Rules & Regulations, Policies & Procedures, applicable written directives, and collective bargaining agreements;
- Not work any details or overtime with exception of court service; and
- Notify their supervisor immediately upon receipt of a subpoena, summons, or other court order. Supervisors shall make every effort to postpone the court date, or provide a substitute witness, where feasible and appropriate. As a last resort, the employee shall appear in court as ordered. Any questions or concerns regarding appearances in court shall be forward to the MSP Legal Section for review.

An employee who is on any form of leave more than thirty (30) days shall return the following issued equipment to their Troop/Section/Unit Commander:

- All issued Department firearms and ammunition;
- All issued Department UOF equipment;
- Assigned vehicle along with vehicle issued equipment;
- Department issued fuel card, transponder and snow gate access cards; and
- All issued electronic devices (e.g., cell phone, laptop computer).

Troop/Section/Unit Commanders shall contact the issuing section regarding storage.

Bereavement Leave

Employees are entitled to leave, without loss of pay or benefits, in recognition of the death of family members or persons living in the household of the employee, in accordance with their respective collective bargaining agreements.

Blood Donation Leave

Employees are permitted a maximum of four (4) hours leave of absence with pay, subject to operational needs and the approval of their supervisor, specifically to enable the employee to donate blood. The decision of their supervisor cannot be appealed.

To qualify for the Blood Donation Leave, an SP 635 Employees Blood Bank form shall be completed certifying the date, location, times and type of blood donation.

Leave time is for:

- Travel from assigned work location to the donation site;
- Actual donation time;
- Recovery from donation; and
- Travel time back to assigned work location.

Leave Time
- Shall be taken on the day the donation occurs;
- Employees shall not accrue compensatory time in lieu of such leave;
- Blood Donation Leave is permitted a maximum of five (5) times per federal fiscal year, the period of October 1 through September 30.

Education Leave

Purpose

Employees may be granted a paid leave of absence for educational purposes to attend conferences, seminars, briefing sessions, or other functions of a similar nature that are intended to improve or upgrade the individual's skills or professional ability.

Request Procedure

A request shall be made in writing to the Leave Coordinator at least forty-five (45) days in advance of the desired leave, or if unforeseen, as soon as possible.

Requests shall include:
- The anticipated start and end dates of training;
- A thorough description of the training accompanied by documentation from the institute hosting the training;
- Rationale for the relationship of the training to the employee's work unit, and/or the Department as a whole; and
- Professional development training requests shall be guided by TRN-01 Training Administration.

Approval

Approval is entirely at the discretion of the Colonel/Superintendent, and is not subject to appeal.

Considerations may include, but not be limited to:
- Costs and benefit of the training to the Department as a whole;
- Benefit of the training to the individual employee and their work unit; and
- The reasonable relationship of the training to the individual employee's work assignment.

Extended Illness Leave Bank (EILB)

EILB is a voluntary program to assist employees who have expended their accrued paid leave due to an extended personal illness or injury, thereby enabling the employee to remain on paid leave within the limits of the program.

Eligibility
- To be eligible for membership, employees shall annually donate an amount of sick, vacation or personal leave credits to the EILB; and
- Apply to withdraw from the EILB, up to one-hundred and twenty (120) days within a two (2) year period, when extended illness or injury have exhausted all their paid leave time.

Note: Employees seeking further information should contact the Leave Coordinator.

Family and Medical Leave (FMLA)

The Department shall grant employees who have completed their probationary period the following Family and Medical Leave in tandem with Workpartners, the absence and leave administrator for the Commonwealth's Executive Department.

Eligible employees may qualify to take leave for these qualifying reasons:

- Bonding with a new child welcomed by birth, adoption, or foster placement;
- For a serious health condition that makes the employee unable to perform the essential functions of their job;
- To care for a family member with a serious health condition;
- To care for a covered servicemember with a serious injury or illness (employee's spouse, child, parent, or next of kin); and/or
- For any qualifying exigency arising out of the fact that an employee's family member is on active military duty or call to covered active-duty status.

Note: Employees shall consult their applicable collective bargaining agreements for specific benefits, durations, definitions, and other information for cited leave.

Request Procedure

Requests shall be made in writing to the Department Leave Coordinator and with Workpartners, by visiting the following website: https://www.mass.gov/info-details/commonwealth-absence-and-leave-management, at least thirty (30) days in advance of the desired leave, or if unforeseen, as soon as possible.

The request shall include the following:

- Your name;
- Your date of birth;
- Your mailing address;
- Your email address (for quicker receipt of documents);
- The start and expected end date of the leave;
- The reason for the leave (including family member name, if relevant); and
- Appropriate documentation (Workpartners will advise on the appropriate documentation needed for the respective leave request.)

Note: Day-to-day sick calls are NOT administered through Workpartners. Employees are required to continue Department protocol for day-to-day sick calls.

Non-FMLA Family Leave

The Colonel/Superintendent may grant employees who have completed their probationary period, Non-FMLA Family Leave in accordance with the appropriate collective bargaining agreement.

Request Procedure

Requests shall be made in writing to the Leave Coordinator at least fourteen (14) days in advance of the desired leave, or if unforeseen, as soon as possible.

The request shall contain the following:

- The anticipated start and end dates of leave, or the intended days for incremental use; and
- The specific reason for the requested leave and any documentation the employee may have in support of the leave request.

Note: Employees shall consult their applicable collective bargaining agreements for specific benefits, durations, definitions, and other information for cited leave.

Paid Family and Medical Leave (PFML)

Paid family and medical leave (PFML) is paid time off of work for family or medical reasons. The Department shall grant employees the following Paid Family Medical Leave in tandem with the Department of Family and Medical Leave (DFML), the PFML administrator for the Commonwealth's Executive Department.

Eligible employees may qualify to take leave for these qualifying reasons:

- Bonding with a new child welcomed by birth, adoption, or foster placement;
- For a serious health condition that makes the employee unable to perform the essential functions of their job;
- To care for a family member with a serious health condition;
- To care for a covered servicemember with a serious injury or illness (employee's spouse, child, parent, or next of kin); and/or
- For any qualifying exigency arising out of the fact that an employee's family member is on active military duty or call to covered active-duty status.

Note: Employees shall consult their applicable collective bargaining agreements for specific benefits, durations, definitions, and other information for cited leave.

Request Procedure

Requests shall be made in writing to the Department PFML Coordinator and with the Department of Family and Medical Leave, by visiting the following website: https://www.mass.gov/how-to/how-to-apply-for-paid-family-and-medical-leave-pfml at least thirty (30) days in advance of the desired leave, or if unforeseen, as soon as possible.

Paid Family and Medical Leave (PFML), continued

The employee shall include the following information on the application:

- The reason you are taking leave;
- The date you notified your employer that you need to take leave; and
- The date when you are planning to take leave, or when your leave started.

Leave of Absence Without Pay

Authorization

The Colonel/Superintendent may grant employees authorized leave of absence without pay for up to ninety (90) days and/or grant an extension of leave of absence upon written request filed by the employee.

Request Procedure

Requests for Leave of Absence Without Pay shall be made in writing to the Leave Coordinator at least thirty (30) days in advance of the desired leave, or if unforeseen, as soon as possible.

- The written request shall contain the following:
  - Anticipated start and end dates of said leave;
  - A detailed statement of the reason for the leave;
  - In the event that the absence is illness/injury related, written requests shall be accompanied by substantiating proof of such illness.

Sworn Members – Return to Service Requirements

The Leave Coordinator shall inform sworn members of any requirements necessary for return to service from leave.

Returning to Service – FMLA-Medical Leave or Authorized Leave of Absence Without Pay:

- Members returning to service due to their own illness/injury that exceeds ten (10) days shall:
  - Notify their Commanding Officer to contact the Occupational Health Unit to schedule an appointment with the State Police Surgeon prior to returning to work; and
  - Have a recommendation from the State Police Surgeon for return to service.

Any leave or break in service 90 days – 1 year:

Members returning from any leave, temporary modified duty or break in service exceeding ninety (90) days requesting full duty status shall ensure the tasks below are completed in the following sequence:

- The members' Station / Section / Unit Commander shall notify Human Resources in advance of date of return and request the member is returned to full duty;
- Human Resources will notify the Division of Standards and Training Commander or designee when the member is returned to full duty;
- The member shall then be required to successfully complete:

- Online academy;
- Refresher training in the following areas (if deemed necessary by the Division of Standards and Training Commander or designee):
    1. Patrol Procedures
    2. Defensive Tactics
    3. EVOC
    4. Firearms (reissuance of assigned UOF gear and requalification if necessary)

- Upon satisfactory completion of training, the Station / Section / Unit Commanders will be advised by the Commandant of the State Police Academy.

Any leave or break in service exceeding 1 year:

Members returning from any leave or break in service exceeding one (1) year requesting full duty status shall ensure the tasks below are completed in the following sequence:

- The members' Station / Section / Unit Commander shall notify Human Resources in advance of date of return and request the member is returned to full duty.
- The member shall then be required to successfully complete:
    - A background investigation;
    - A medical examination by the State Police Surgeon to include drug testing; and
    - Psychological testing.

Sworn Members – Return to Service Requirements, continued

Human Resources will notify the Division of Standards and Training Commander or designee when the member is returned to full duty.

The member shall then be required to successfully complete:

- Online academy
- Refresher training in the following areas (if deemed necessary by the Division of Standards and Training Commander or designee):
    - Patrol Procedures
    - Defensive Tactics
    - EVOC
    - Firearms (reissuance of assigned UOF gear and requalification if necessary)
- Upon satisfactory completion of training, the Station / Section / Unit Commanders will be advised by the Commandant of the State Police Academy.

Former members wishing to return from a separation from service that exceeds three (3) years shall:

- Meet all requirements for re-entry to the Department; and
- Successfully complete the Recruit Training for appointment to the position of Trooper.

Note: Failure to successfully complete the Recruit Training may affect pension benefits, if applicable.

Returning From Leave: Civilians

Return From Leave

- Civilian employees returning from a leave that exceeds one (1) year shall be required to successfully complete:
  - A background investigation;
  - A drug test;
  - A medical examination by the State Police Surgeon, as applicable, if returning from medical leave where the employee was the one that was ill; and
  - Retraining, as determined by the employee's supervisor or the Human Resources Director.

Sworn Members Returning From Disability

In addition to the previously listed requirements, sworn members returning from disability retirement shall have a medical evaluation conducted in conformance with M.G.L. c. 32, and the standards of the Commonwealth of Massachusetts Public Employee Retirement Administration Commission.

Benefits

Employees may be required to pay premiums for certain benefits while on leave.

Military Leave

Refer to Policy and Procedure ADM-26 Military Service.

References:

Code of Massachusetts Regulations 458 (CMR) 2:00: Department of Family and Medical Leave;
M.G.L. c. 175M Family and Medical Leave;
M.G.L. c. 31, § 37;
M.G.L. c. 32;
NAGE Units 1, 3 and 6-Commonwealth CBA, Article 8;
AFSCME Unit 2-Commonwealth CBA, Article 8;
SPAM Unit 5A-Commonwealth CBA, Articles 8 and 38;
MOSES Unit 9-Commonwealth CBA, Article 8;
Personnel Administrator Rules, PAR 13 Leaves of Absence;
Red Book §§5.00, 6.00, and 8.00;
Massachusetts State Employees Blood Program;
MPAC 22.2.0.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**ADM-12**
Subject:	
Serious Injury/Death of a Member	

Policy

The Department recognizes that the death or serious injury of a member is traumatic and shall provide assistance to the member's family, recognizing that the needs of the family generally take precedence over the wishes of the Department.

Department members shall:
- Ensure that whenever a member's next of kin calls, their questions are answered honestly and openly.

OFF-DUTY Death Notification Procedure

When any member becomes aware of the death of a current or retired member of the Department of State Police, or an immediate member of their family, they shall immediately:
- Notify the Office of the Superintendent through channels.

Information for notification shall include:
- Personal information on the deceased person;
- The circumstances of the death;
- Any funeral arrangements; and
- A family contact person.

The Office of the Superintendent shall notify:
- Members of the Department; and
- Special effort shall be made to contact the member's graduating class.

ON-DUTY Death Notification Procedure

If the death or life threatening injury occurs on-duty, the member's Commanding Officer or designee shall immediately notify:
- The Office of the Superintendent.

The Colonel/Superintendent shall immediately:
- Assign a ranking member to personally contact the member's immediate family; however
- Every effort shall be made to use a member of the Department who is a personal friend, along with the ranking member.

Liaison Member

If the family chooses, the Colonel/Superintendent shall:

- Appoint a Department member as a liaison, to provide additional assistance to the immediate family of the deceased/injured member or retiree.

As a guide, the liaison member should:

- Assist the family in contacting clergy, friends, and relatives;
- Assist the family with funeral arrangements;
- Provide transportation assistance for the immediate family;
- Arrange for security needs of the home and screening of phone calls prior to and on the day of the funeral;
- Coordinate the family's efforts to determine the status and amounts of compensation to which the deceased member may be entitled; and
- Keep the Colonel/Superintendent informed of all arrangements and developments.

Honor Guard

The Colonel/Superintendent shall:

- Designate a member to be the Officer-in-Charge (OIC) of the funeral detail.

The OIC shall:

- Coordinate with the liaison member; and
- Adhere to GEN-04A Ceremonial Tributes regarding funeral details.

References: GEN-04A Ceremonial Tributes;
SUP-04 Employee Assistance Unit.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**ADM-13**

Subject:

Notification of Medical Examiner and/or Next of Kin

Policy

The Department shall promptly and compassionately notify the nearest relative of victims who have sustained life threatening injuries, or passed away.

Notification of Medical Examiner

The Medical Examiner (ME) of jurisdiction shall be notified whenever a member of the Department becomes aware of a death (Specific circumstances appear in MGL c.38, §4, 6.).

Responsibilities

Note: The District Attorney's Office or State Police Detective Unit (SPDU) of jurisdiction shall direct the investigation of all homicides, suicides, and unattended deaths (including traffic fatalities, as requested by the Office of the District Attorney of jurisdiction).

Position	Duties
First member at the scene	• Notify the Barracks Desk Officer. • For all homicides, suicides, and unattended deaths, secure the scene, pending arrival of the SPDU of jurisdiction.
Station Desk Officer	• Immediately notify the Troop Duty Officer.
Troop Duty Officer	Immediately notify the appropriate: • SPDU of jurisdiction of all homicides, suicides, and unattended deaths, and take any action requested; and • Local ME Office, as requested by SPDU. If the ME declines to respond to the scene, request authority from the ME to remove the body. If the ME is unavailable, contact the Office of the Chief Medical Examiner at (617) 267-6767 and request authority to remove the body.
Troop Commanders	Ensure that their Troop Duty Office has an updated list of Medical Examiners' phone numbers and addresses.

Next of Kin

Every effort should be made to locate the next of kin in the order of:

- Live-in spouse;
- Parents or legal guardian;
- Adult children;
- Brother or sister; or
- Other relatives.

Request for Notification

Members may be called upon to notify the next of kin that a family member or friend has been seriously injured or is deceased. Except under unusual circumstances, **this notification should be made in person.** No identifying information of the victim or their family shall be transmitted via radio.

Position	Responsibility

Members receiving request to notify the next of kin	• Request as much information as possible, to include:
	  o Cause of death and/or injuries;
	  o Location of deceased or injured person; and
	  o Contact person and telephone number.
	• If the member is unfamiliar with the caller, seek to confirm the information.
	• Notify Troop Duty Officer.

Troop Duty Officer	• Notify the appropriate Detective Unit of all homicides, suicides, and unattended deaths (including traffic fatalities if so requested by the DA's Office of jurisdiction). • Determine who shall make the notification to the next of kin. • If the notification is not to be made in person, determine what means shall be used.

District Attorney Offices

Whenever there is a homicide, suicide, or unattended death, the Division of Investigative Services shall determine the notification process. Members assigned to an Office of a District Attorney shall follow the protocols promulgated for their particular office.

All other notifications shall be made by the Division of Field Services.

Field Services Procedure

Whenever possible, two (2) members shall be sent to make a notification of serious injury, illness, or death.

The member who is making the notification should carefully prepare their message before speaking with the next of kin. When possible, members shall:

- Seek assistance from clergy, relative, or close friend of the family;
- Make the notification in a private setting, and ask the recipient to sit down;
- Deliver the information to the recipient in a gradual manner;
- Observe the recipient carefully as the information is given;
- If possible, do not leave the recipient alone. Members should attempt to contact a relative, friend, or neighbor to stay with the recipient; and
- When the recipient is operating a motor vehicle, the member shall ascertain if they are able to continue driving. If not, members may transport or make transportation arrangements for the recipient.

References: MGL c.38, §4, 6.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**ADM-14**
Subject:	
Internal Department Investigations	

Policy

To protect the integrity of the Department and to ensure continued public support:

- All Department employees shall adhere to the Department's Policies and Procedures regarding external complaints (including anonymous complaints) against any employee, or involving any policy, procedure, or operation of the Department;
- All complaints shall be documented and investigated according to complaint intake procedures;
- Complaints, when assigned, shall be investigated at the lowest appropriate organizational level, unless determined otherwise by the Division of Standards and Training (DST) Commander or designee;
- All complaints against Department employees and/or the Department shall be maintained in a secure manner to protect confidentiality;
- The withholding of officers' disciplinary records related to a misconduct investigation as a public records exemption is prohibited;
- Access shall be provided to the Peace Officer Standards and Training Commission's (POST) Division of Police Standards to audit all records related to complaints, investigations, and personnel records pursuant to the rules and regulations promulgated by POST;
- The DST Division Commander, or designee, shall transmit any officer misconduct complaint received by the Department in accordance with MGL c.6E § 8(b) within 2 business days to the division of police standards in accordance with POST requirements;
- The DST Division Commander shall notify the Colonel/Superintendent of complaints against Department employees and/or the Department.
  - Immediate notification shall be made in cases involving allegations of serious misconduct.
  - Weekly reports shall be provided verbally on all other complaints or involving complaints against a sworn member;
- DST shall comply with the investigation and notification requirements of MGL c. 6E, § 8(b) and §10(h); and
- The Colonel/Superintendent shall have the authority to conduct and/or direct an inquiry as necessitated by circumstance.

Definition

Internal Investigation: An investigation or inquiry related to complaints against Department policy, procedure or operations.

Personnel Investigation: An investigation or an inquiry into the actions of an employee that may result in charges of misconduct.

Rights of the Accused Employee

An accused employee shall:

- Receive a copy of the complaint, including the name of the complainant, if known, prior to any employee interrogation;
- Be afforded full constitutional and other legal protections; and
- Be afforded the appropriate protections under applicable collective bargaining agreements.

Rights of the Complainant

The Complainant shall be:

- Notified of the receipt of the complaint, and the steps to be taken;
- Given a status report when requested; and
- Notified of the final disposition classification.

Use of Examinations

If, during an investigation, it becomes necessary to request an employee to submit to an examination or required test(s), the Troop/Section/Unit Commander shall contact DST for approval.

The results of medical tests shall be afforded appropriate privacy rights according to applicable laws.

Complaint Intake Procedures

A complaint that requires <u>immediate attention</u> shall:

- Be immediately referred to the Troop/Section/Unit Commander, Duty Officer or Shift Supervisor.

<u>External Complaints</u>

External complaints are to be completed by the Complainant on a SP 340 Public Response Form. The Complainant may obtain a SP 340 by:

- Contacting a State Police facility for instructions;
- Arriving in person to a State Police facility and securing a copy of a SP 340;
- Downloading the SP 340 form from the State Police external website http://www.mass.gov/msp or https://www.mass.gov/how-to/submit-a-public-response-report ; or
- Calling the Public Response Intake Line (508) 988-7003 and following the prompts.

Complaint Intake Procedures, continued

When a Complainant calls or arrives at a State Police facility the following shall occur:

- The Desk Officer or employee who attends to a Complainant, either by telephone or in person, shall:
  - If applicable to their work assignment, log only the name and address of the Complainant into the Daily Administrative Journal (DAJ) (the Complainant should not be asked to identify the employee(s) named in the complaint, nor should any employee information pertaining to this complaint be included within the DAJ entry). Note: DAJ information would also include anonymous complaints or when the Complainant refuses to give his/her name;
  - Give the Complainant a copy of the SP 340 form; or
  - Instruct the Complainant on how to obtain a SP 340 form from the above options;
  - Ensure the Complainant understands all options and the submission procedure; and
  - Assure the Complainant that all complaints shall be addressed by the Department.

In instances where the Complainant demands to immediately speak to a supervisor the following shall occur:

- Division of Field Services employees shall notify the Troop Duty Officer of jurisdiction and then refer or forward the Complainant to the same Troop Duty Officer; or
- Division of Investigative Services, Division of Administrative Services, Division of Standards and Training, and Division of Homeland Security and Preparedness employees shall notify a Commissioned Officer from within their Division and then refer or forward the Complainant to the same Commissioned Officer.

The Troop Duty Officer or the Division Commissioned Officer shall:

- Record the Complainant within the DAJ, if applicable to his/her work assignment. Note: DAJ information would also include anonymous complaints or when the Complainant refuses to give his/her name;
- Explain the complaint intake procedure to the Complainant;
- Instruct the Complainant on how to obtain a SP 340 form from the above options; and
- Assure the Complainant that all complaints shall be addressed by the Department.

Employees who receive complaints about their own conduct shall immediately:

- Notify their Troop Duty Officer or a Commissioned Officer within their Division; and
- Transfer or refer the Complainant to the same Troop Duty Officer or Commissioned Officer within their Division.

Complaint Intake Procedures, continued

Internal Complaints

Internal personnel complaints originating within the Department by any employee shall be documented in a To/From format. The To/From shall be submitted in the following manner:

- Copy faxed or emailed to DST within twenty-four (24) hours from the date of the To/From;
- Copy submitted through channels to the appropriate Troop/Section/Unit Commander; and
- Original forwarded to DST.

SP 340 Public Response Form Submission

SP 340 Public Response Form shall be submitted in the following manner:

- Delivered in person to the Massachusetts State Police General Headquarters, 470 Worcester Road Framingham, MA 01702 / Public Response Reports; or
- Faxed to: The Division of Standards and Training / Public Response Reports (508) 820-2149; or
- Emailed to: The Division of Standards and Training/ Public Response Reports at publicresponsereports@pol.state.ma.us; or
- Mailed to: The Massachusetts State Police Division of Standards and Training/ Public Response Reports, 470 Worcester Road Framingham, MA 01702.

Interviews

For all interviews, reasonable arrangements shall be made to accommodate the schedules of the parties involved.

Interviews may be recorded mechanically or by a Department stenographer. The accused employee may independently record his/her own interview.

Investigation

Step	Action
1	Supervisors shall conduct assigned investigations within thirty (30) days.
2	The complaint shall be categorized as: • Employee's conduct; • Validity of the enforcement action taken; • Department policy, procedure, or operations; or • Other.
3	The investigating member shall make a conclusion of fact for each complaint, which shall be reviewed by the appropriate Troop/Section/Unit Commander. Dispositions shall be classified as: • **Unfounded** - Complaint or incident is false and not factual. • **Exonerated** - Incident occurred, but employee's action was lawful and proper. • **Not Sustained** - Insufficient evidence to prove or disprove the complaint. • **Sustained** - The complaint or incident is supported by sufficient evidence to prove employee misconduct.

4	Complaint dispositions classified as **Unfounded**, **Exonerated, or NOT- Sustained,** and not alleging serious misconduct, shall be filed within the Internal Affairs database. For **Sustained** disposition classifications the Troop/Section/Unit Commander shall: • Prepare a memorandum indicating the category of the complaint, and recommendations; and • Forward the memorandum, with all completed reports and correspondence, through channels to DST.
5	The affected employee and Complainant shall be notified of the final disposition classification by the Troop/Section/Unit Commander or the DST Commander.

Note: Nothing in this policy should prevent members from taking appropriate and timely action for any allegations of criminal activity or criminal acts.

Responsibilities

Position	Duties
All Employees	• Follow the complaint intake procedures; and • Ensure the Complainant understands: o All options for acquiring a SP 340; o The SP 340 submission procedure; and o That all complaints shall be addressed by the Department.
Supervisor	• Follow the complaint intake procedures; and • Review complaints and conduct investigations when assigned.
Troop Duty Officer or Division Commissioned Officer	• Follow the complaint intake procedures; and • Ensure the Complainant understands: o All options for acquiring a SP 340; o The SP 340 submission procedure; and o That all complaints shall be addressed by the Department.
Troop/Section/Unit Commander	• Initiate investigations on complaints about employees under their supervision or command as assigned by DST; and • Forward completed reports and recommendations to the DST Division Commander within thirty (30) days of assigned date. Note**:** DST may authorize a time extension upon a written request.
Complaint Intake Officer	• Process SP 340 received according to standards established by DST.

Office of Professional Integrity and Accountability	• Provide oversight of all personnel investigations in accordance with the Section's Standard Operating Procedure (SOP).
Division Commander	• Review investigative reports; • Forward recommendations and requests for disciplinary action to DST; and • Issue letters of counseling as appropriate.

Responsibilities, continued

Position	Duties
Division of Standards and Training	• Review complaints in accordance with the Division's SOP; • Notify the Division Commanders of any personnel investigations conducted by Office of Professional Integrity and Accountability; and • Review recommendations for disciplinary action with the Deputy Superintendent.
Deputy Superintendent	• Review recommendations for disciplinary action with DST; and • Administer disciplinary action as appropriate which has been approved by the Colonel.
Colonel/Superintendent	• Refer personnel investigations to entities outside the Department, as necessary; and • Review, prescribe and impose discipline.

References: ADM-15 Office of Professional Integrity and Accountability;
MGL c. 6E, § 8(b), §10(h);
SP 340 Public Response Form;
Carney v. Springfield, 404 Mass 604 (1988);
Kastigar v. U.S., 406 US 441 (1972);
Garrity v. NJ, 385 US 493 (1967);
Collective Bargaining Agreement(s);
MPAC: 52.1.1, 52.1.2, 52.2.1, 52.2.2, 52.2.3, 52.2.4, 52.2.5, 52.2.6, 52.2.8, 52.2.9.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**ADM-15**

Subject:

Office of Professional Integrity and Accountability Investigations

Policy

The Office of Professional Integrity and Accountability (OPIA) investigates allegations of serious misconduct by employees of the Department or as ordered by the Office of the Superintendent (OS) or the Division of Standards and Training (DST).

In accordance with MGL c. 6E, § 10(h), OPIA shall complete an internal affairs investigation into officer misconduct and issue a final disposition within one year of receiving a complaint or notice from the POST commission of the complaint being filed. The POST commission may, upon a showing of good cause, extend the time to complete the investigation upon notification from OPIA.

Organization

OPIA has the authority to report directly to the OS.

Serious Misconduct

Serious misconduct includes, but is not limited to, acts of:

- Corruption;
- Criminal conduct;
- Use of excessive force; and
- Civil rights violations.

Jurisdiction

Complaints are investigated at the lowest appropriate organizational level in accordance with ADM-14 Internal Department Investigations.

OPIA may investigate any complaint when:

- Requested by the Troop/Section/Unit Commander, with approval from DST;
- Directed by the OS or DST; or
- The complaint alleges serious misconduct.

The Colonel/Superintendent shall have the authority to conduct and/or direct an inquiry as necessitated by circumstance.

Use of Examinations

Upon the approval of the DST Commander or designee, any employee subject to an internal investigation may be asked to submit to tests, examinations, and/or disclosures. These procedures may include, but are not limited to, the following:

- Ballistics and chemical tests;
- Submission to photographing;
- A photograph array or line-up;
- Forensic and polygraph examinations;
- Financial disclosure statements;
- Audio/video recordings; and
- Medical and/or laboratory examinations.

Examinations and/or tests shall be:

- Relevant and material to the subject investigation;
- Specifically directed and narrowly related to such investigation; and
- Completed within a reasonable time and according to professionally accepted standards.

For Internal Affairs Investigations, a polygraph examination may only be used in investigations of criminal conduct.

The results of medical tests shall be afforded appropriate privacy rights according to applicable laws.

Procedure for OPIA Cases

Step	Action
1	Open an OPIA case file.
2	Notify the affected employee in writing regarding: • The nature of the investigation; • The employee's rights as legally required; and • The employee's responsibilities relative to the investigation. NOTE: The OPIA can request written authorization from DST not to notify the employee if the notification could hinder the investigation. However, the employee must be informed of the nature of the investigation before any interrogation takes place of the employee.
3	Provide notification to the employee's Commanding Officer, unless it would hinder the investigation.
4	Conduct the investigation in a timely manner.
5	Prepare a report on the investigation for DST, with supporting facts for each allegation and a classification of the complaint: • Unfounded; • Exonerated; • Not Sustained; or • Sustained.
6	In accordance with MGL c.6E §8(b) DST shall act as the designee of the Colonel. Upon completion of the internal investigation of a complaint DST shall immediately transmit to the POST Commission division of police standards an

	investigation report in a form determined by the commission. Further, upon the final disposition of the complaint, DST shall immediately transmit to the division of police standards a final report in a form to be determined by the Commission.
7	The DST Commander shall notify the affected employee in writing, through channels, of the decision(s).
8	All case files shall be permanently retained.

References: ADM-09A Staff Inspections;
ADM-14 Personnel Investigations;
MGL c. 4, § 7 and c. 66A, § 2;
MGL c.6E, §8(b);
Furtado v. Town of Plymouth, 451 Mass 529 (2008);
MPAC: 52.1.3, 52.2.1, 52.2.3, 52.2.5, 52.2.6, 52.2.8, 52.2.9.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**ADM-16**

Subject:

Notifying Prosecuting Agencies Regarding Evidence

Policy

Prosecuting agencies shall be notified of any and all Departmental investigations, to include personnel and/or internal affairs investigations associated with an open criminal prosecution or investigation. Department members who generate records, percipient witness statements, and/or evidence that relate to a criminal prosecution shall and must notify the appropriate agency prosecuting the case. The assigned lead Departmental investigator in any criminal or administrative investigation is responsible for ensuring such notification is made.

Definitions

Internal Affairs Investigation: Any investigation conducted pursuant to ADM-15 Internal Affairs Investigations.

Personnel Investigation: Pursuant to ADM-14 Personnel Investigations, any investigation or inquiry into the actions of an employee that may result in charges of misconduct.

Reporting

A Department investigator assigned to an investigation, to include personnel and/or internal affairs investigations, shall:

- Determine whether the investigation to which he or she is assigned relates to the same facts and circumstances of an open criminal prosecution or investigation;
- Notify the agency prosecuting the open criminal matter of the related Departmental investigation; and document the same in official Department records;
- Upon request of the prosecuting agency, provide any related Departmental records, percipient witness statements and/or evidence to said prosecuting agency, and advise their supervisor and the State Police Legal Section of documents/evidence being provided. The Legal Section will document and maintain a record of the documents or evidence that were provided;
- If the lead investigator believes such notification may adversely affect the investigation to which they are assigned, they shall immediately address the same in writing through their chain of command with a final determination documented in official Department records.

Subject:	Number:
Notifying Prosecuting Agencies Regarding Evidence	**ADM-16**

References: ADM-14 Personnel Investigations;
ADM-15 Internal Affairs Investigations;
Brady v. Maryland, 373 U.S. 83;
Commonwealth v. Tucceri, 412 Mass. 401;
Commonwealth v. Wanis, 426Mass. 639.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**ADM-17**

Subject:

Employee Evaluation System

Policy

The Department shall continuously maintain an Employee Evaluation System (EES) to establish and measure performance expectations for sworn members.

The EES shall be conducted in accordance with the Department's EES Manual.

EES Coordinator

The EES Coordinator shall be a Commissioned Officer or Program Coordinator designated by the Division Commander of Standards and Training or designee.

EES Purpose

EES is a proven tool for continuous individual and organizational improvement. Some primary purposes of EES are to:

- Maintain continuous supervisor/employee lines of communication and feedback;
- Motivate employees to improve by understanding their needs;
- Establish goals and objectives at all organizational levels;
- Evaluate the quality of performance; and
- Evaluate the readiness to handle enhanced responsibilities.

References: MGL c. 22C, § 22;
Department of State Police Employee Evaluation System Manual.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**ADM-18**

Subject:

Unlawful Harassment, Sexual Harassment and Discrimination

Policy

The Department shall promote and maintain a working environment free from unlawful harassment, sexual harassment and discrimination.

Purpose

This policy addresses all forms of sexual harassment and addresses discrimination and unlawful harassment based on race, color, religious creed, national origin, age (40 or older), sex (including pregnancy), gender identity or expression, sexual orientation, genetic information, ancestry, handicap (disability), protected veteran status, participation in discrimination complaint-related activities or other protected class under law.
Note: The definitions found in 804 CMR 3.00, et seq., as amended (the MCAD's *Employment Discrimination Guidelines*), shall be applicable to, and are hereby incorporated into, this policy.

This policy does not address conduct, conflicts, or disagreements otherwise addressed through the chain of command or within Department Policy and Procedures. Internal complaints or concerns, which do not relate to an identified protected class or sexual harassment, will not be addressed under this policy. Such complaints may have another course of action such as in ADM-14 Personnel Investigations or SUP-12 Office of the Ombudsman.

Harassment Investigation Unit (HIU)

The Sexual Harassment Officer for the Department is the Division Commander of Standards and Training.

Harassment Investigation Officer(s) shall be Commissioned Officer(s) assigned by the Colonel/Superintendent and shall report to the Division of Standards and Training.

All Complaint Forms of unlawful harassment, sexual harassment or discrimination shall be forwarded to the Harassment Investigation Unit (HIU). Upon receipt of such such complaint form, the HIU shall perform an intake and may make recommendations for various avenues of resolutions. If the HIU determines an investigation is required, the complaint shall be forwarded to the Commonwealth's Human Resources Division's Investigations Center of Expertise (COE) for investigation and findings. All HIU investigations shall remain confidential to the extent practicable. All Supervisors (except for Supervisors assigned to the Office of the Ombudsman and/or Employee Assistance Unit) shall immediately report

Harassment Investigation Unit (HIU), continued

incidents of unlawful harassment, sexual harassment or discrimination to the Harassment Investigation Unit.

Discrimination Defined

Discrimination is the unequal and unlawful treatment of persons ***in employment related decisions*** because of race, color, religious creed, national origin, age (40 or older), sex (including pregnancy), gender identity or expression, sexual orientation, genetic information, ancestry, handicap (disability), protected veteran status, participation in discrimination complaint-related activities and/or other protected class under law.

Discrimination Examples

Conduct may include, but is not limited to, when the Department:

- Bases employment decisions solely on the race of an applicant; or
- Makes assignments solely on the age of an employee.

Unlawful Harassment Defined

Unlawful harassment is unwelcome conduct that is based on race, color, religious creed, national origin, age (40 or older), sex (including pregnancy), gender identity or expression, sexual orientation, genetic information, ancestry, handicap (disability), protected veteran status, participation in discrimination complaint-related activities and/or other protected class under law.

Harassment becomes unlawful when:

- Enduring the offensive conduct becomes a condition of continued employment; or
- The conduct is severe or pervasive enough to create a work environment that a reasonable person would consider intimidating, hostile, or abusive.

Unlawful Harassment Examples

Conduct may include, but is not limited to:

- Offensive jokes, slurs, epithets or name calling, or other derogatory comments;
- Physical assaults or threats, intimidation, ridicule or mockery, insults or put-downs, or other verbal or physical conduct that denigrates or shows hostility or aversion; or
- Objects, photographs, images, or demeaning gestures connected to an individual's membership in a protected class.

Sexual Harassment Defined

Sexual harassment is unwelcome sexual conduct such as: sexual advances, requests for sexual favors, and/or other verbal or physical conduct of a sexual nature, when:

Sexual Harassment Defined, continued

- Submission to or rejection of such advances, requests or conduct is explicitly or implicitly made a term or condition of employment or as a basis for employment decisions;
- Such advances, requests or conduct have the purpose or effect of unreasonably interfering with an individual's work performance; or
- Such advances, requests or conduct have the purpose or effect of creating an intimidating, hostile, humiliating, or sexually offensive work environment.

It is not necessary to meet the threshold of sexual harassment as defined by law to be considered a violation of this policy.

Sexual Harassment Examples

Examples of sexual harassment, may include but are not limited to:

- Direct sexual advances or assaults;
- Sexual inquiries, jokes, and epithets;
- Derogatory comments about a person's sex, sexual orientation or gender identity or expression;
- Other forms of verbal abuse of a sexual nature, such as whistling or catcalling;
- Offensive or unnecessary touching, pinching, patting, etc.;
- The display of sexually suggestive posters, photographs, or objects; or
- An employee receiving job benefits contingent on sexual favors (quid pro quo).

Sexual Harassment Victims

Victims of sexual harassment <u>may</u> be…	**The harasser <u>may</u> be…**
Of the same or different gender as the harasser.	Of either gender.
A third person who is not the intended target of the sexual harassment or conduct.	Any employee or in certain circumstances someone who is not an employee (vendors, contractors).

Liability and Sanctions

Employees may be personally liable if they engage in unlawful harassment, sexual harassment or discrimination.

Any employee found to have engaged in unlawful harassment, sexual harassment, or discrimination in violation of this policy is subject to disciplinary action up to and including termination.

Supervisors may potentially be personally liable if they knew or should have known about incidents of sexual harassment, and did not take appropriate corrective action.

The Department may not be held responsible in cases of unlawful harassment, sexual harassment, and/or discrimination, if it can show that it took prompt and appropriate corrective action.

Complaint Procedure

Step	Action
1	Process for reporting incidents of unlawful harassment, sexual harassment, discrimination, and/or retaliation: • Notify a supervisor, who shall assist in reporting the complaint to the Harassment Investigation Unit (HIU); • Fax a copy of the SP 387 *Unlawful Harassment, Sexual Harassment and Discrimination Complaint* Form directly to the HIU at (508) 820-2149, or email to MSPHIU@MASSMAIL.STATE.MA.US; • Forward the original SP 387 to the HIU 470 Worcester Road, Framingham, MA 01702; • Report Complaint to the Director of Human Resources at GHQ, who shall forward to the HIU; • Report Complaint to the Diversity Office of the Office of Diversity and Equal Opportunity, who shall forward to the HIU; and • Report Complaint to the Chief Legal Counsel, who shall forward to the HIU.
2	The HIU shall promptly: • Respond to the complainant; • Review all available information pertaining to the complaint; • Determine if the aggrieved individual(s) is/are a member of a class protected under the law and this policy; • Determine if the alleged conduct meets the definition of unlawful harassment, sexual harassment or discrimination as defined in this policy; • Perform an intake and may make recommendations for various avanues of resolutions where appropriate; • If the HIU determines an investigation is required, the complaint shall be forwarded to the Commonwealth's Human Resources Division's Center of Expertise for investigation and findings; • To the extent practicable, ensure that all interviews by HIU are digitally recorded.; • Consult procedures included within the Department's Resolution Process as outlined within the Affirmative Action Plan; and • Make a report of findings and forward report to the Commander of the Division of Standards and Training. Consistent with Commonwealth and Department Policy/Rules and Regulations, and in a manner determined by the Division Commander of Standards and Training, HIU completed confidential reports will be made available for inspection to complainants and persons alleged to have committed unlawful

Complaint Procedure, continued

	harassment, sexual harassment, discrimination and/or retaliation upon request.

3	An employee may also file a complaint with: **Human Resources Division's Investigations Center of Expertise (COE)** **www.mass.gov/service-details/investigations-center-of-expertise** **Phone: 833-778-7270** **E-mail: HRDInvestigations@mass.gov** **Massachusetts Commission Against Discrimination (MCAD)** www.mass.gov/mcad Main Office: One Ashburton Place, Room 601, Boston, MA 02108 Phone 617-994-6000 TTY: 617-994-6196 Regional Offices New Bedford Office: 800 Purchase Street, Room 501, New Bedford, MA 02740 Phone: 508-990-2390 Springfield Office: 424 Dwight Street, Rm. 220, Springfield , MA 01103 Phone 413-739-2145 Worcester Office: 484 Main Street, Room 320 Worcester, MA 01608 Phone 508-453-9630 **Office of Diversity and Equal Opportunity** One Ashburton Place, Room 213 Boston, MA 02108-1516 Telephone 617-727-7441 (Note: this office takes only **Discrimination** complaints.) **US Equal Employment Opportunity Commission (EEOC)** www.eeoc.gov John F. Kennedy Federal Building 475 Government Center, Boston, MA 02203 Phone: 1-800-669-4000 TTY: 1-800-669-6820

4	The Harassment Investigation Unit shall notify the Department's Office of Diversity and Equal Opportunity of complaints of unlawful harassment or discrimination.

Responsibilities

Position	Duties
Supervisors	• Aggressively monitor the workplace to prevent and detect unlawful harassment, sexual harassment, and discrimination; • Take appropriate corrective action to stop all types of unlawful harassment, sexual harassment, and discrimination; • Immediately report incidents of unlawful harassment, sexual harassment, or discrimination to the Harassment Investigation Unit; • Assist any employee in filing a complaint, or obtaining information on the Commonwealth's Sexual Harassment Policy; and • Contact the HIU for information and guidance pertaining to unlawful harassment, sexual harassment and/or discrimination.
All Employees	• Shall not engage in any harassment, sexual harassment, or discrimination; • Shall cooperate in investigations of any harassment, sexual harassment, and discrimination; • Shall actively participate in the Department's efforts to prevent and eliminate any harassment, sexual harassment, and discrimination; and • May contact the HIU for information and guidance pertaining to any harassment, sexual harassment and/or discrimination.

Office of the Ombudsman/ Employee Assistance Unit

All employees should be aware that conversations with the Office of the Ombudsman and/or Employee Assistance Unit are considered confidential and are not the proper venue to notify the Department of unlawful harassment, sexual harassment and/or discrimination complaints. Supervisors assigned to the Office of the Ombudsman or the Employee Assistance Unit are not required to report such complaints through the official chain of command.

Retaliation

Any retaliation against an individual who has complained about unlawful harassment, sexual harassment, discrimination or for cooperating with a complaint and/or investigation of harassment, sexual harassment, or discrimination is unlawful and shall not be tolerated. Any such retaliation shall be a violation of this policy. Incidents of such retaliation shall be reported to the HIU in To/From format.

Subject: **Unlawful Harassment, Sexual Harassment and Discrimination**	Number: **ADM-18**

Distribution of Policy

This policy shall be issued to each employee upon hiring and to all employees annually thereafter. This policy shall be continuously posted and available on DocuShare.

Statewide Policy

The Department shall adhere to the Commonwealth of Massachusetts Human Resources Division Sexual Harassment Policy.

Findings

In the event that an investigation is conducted regarding unlawful harassment, sexual harassment, discrimination, and/or retaliation, the findings shall be classified as one of the following:

- ***Unfounded*** - Complaint or incident is false and not factual;
- ***Exonerated*** - Incident occurred, but employee's action was lawful and proper;
- ***Not Sustained*** - Insufficient evidence to prove or disprove the complaint; or
- ***Sustained*** - Complaint or incident is supported by sufficient evidence to prove employee misconduct.

Cases in which the complainant has withdrawn the complaint shall be classified as Withdrawn. Cases that are approved for an alternate resolution shall be classified as referred. In all cases, a record shall be made in the case file. All findings, withdrawals and referrals shall be reviewed and approved by the Division Commander of Standards and Training.

Any complaint which is sustained shall be deemed a violation of ADM-18 and/or the Rules and Regulations of this Department and shall be handled in accordance with Rules and Regulations of the Department, as applicable. Whether found to be a violation of ADM-18 or not, any inappropriate employee conduct, including but not limited to making or providing false claims, reports, information, statements and/or testimony, may be deemed a violation of Department Policy/Rules and Regulations and is subject to investigation under ADM-14 Personnel Investigations. All investigations shall be conducted in accordance with ADM-14 Personnel Investigations.

<u>NOTE</u>: Nothing in this policy should prevent members from taking appropriate and timely action for any allegations of criminal activity or criminal acts.

Subject:	Number:
Unlawful Harassment, Sexual Harassment and Discrimination	**ADM-18**

References:
ADM-14 Personnel Investigations;
ADM-36 Diversity and Equal Opportunity;
SUP-04 Employee Assistance Unit;
SUP-12 Office of the Ombudsman;
MGL c.l5lB, §3, 3a, and 4;
MGL c.214, §1c;
804 CMR 3.00 Employment Discrimination Guidelines;
MCAD Model Sexual Harassment Policy;
US Equal Employment Opportunity Commission Regulations and Guidance;
Department Rules and Regulations;
Department of State Police Affirmative Action Plan;
Executive Order 526- Order Regarding Non-Discrimination, Diversity, Equal Opportunity, and Affirmative Action;
Commonwealth of Massachusetts HRD Sexual Harassment Policy;
Title VII of the Civil Rights Act of 1964;
SPAM Collective Bargaining Agreement Article 27;
SP 387 Unlawful Harassment, Sexual Harassment and Discrimination Complaint form.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**ADM-19**
Subject:	
Vehicle Management	

Policy

To establish a central management system for all vehicles owned or controlled by the Department in order to maintain a state of operational readiness.

Procurement

The Fleet Administrator shall authorize and be responsible for the procurement of all Department vehicles including:

- Vehicle specifications;
- Bidding processes; and
- Equipment, parts and materials necessary for vehicle maintenance.

Fleet Administrator

The Fleet Administrator shall:

- Maintain a master vehicle inventory for computer/cruiser number, operator, operator assignment, vehicle model year, mileage, registration number, and condition;
- Ensure the annual reconciliation of the master inventory during the month of June;
- Maintain a sufficient inventory of parts, materials, and equipment at Fleet and Troop/Section garages, subject to available funding;
- Issue parts and materials to Troop/Section garages according to need and availability;
- Maintain detailed vehicle maintenance records; and
- Notify Department personnel of manufacturer vehicle recalls.

Fleet Coordinator

Troop/Section Commander or designee shall act as the Fleet Coordinator, and shall:

- Ensure that monthly mileage and state inspections are submitted through established Departmental procedures.

Specialty Vehicles

Requests for specialized vehicles shall be forwarded through the respective Division Commander to the Fleet Administrator.

Specialty vehicles shall:

- Be purchased based on needs of the Department;
- Be assigned to personnel within the specialized sections/units;
- Follow the operational guidelines set forth in ADM-19A Vehicle Use and Maintenance; and
- Remain within the assigned section/unit unless otherwise authorized by the Fleet Administrator.

Vehicle Status

Designation	Meaning
Active	Assigned and in-use
Down*	Inoperable, requires repairs
Out of Service*	Permanently disabled
Spare	Unassigned and available for use
*Vehicles designated "Down" or "Out of Service" **shall not be operated**.	

Vehicle Assignment

The Fleet Administrator or designee shall:

- Maintain control over vehicle assignment and re-assignment;
- Assign vehicles based on the year, condition, and mileage;
- Assign vehicles to individual personnel based upon availability and particular assignment; and
- Prior to the assignment or replacement of a vehicle:
  - Analyze inventory reports of affected vehicle(s);
  - Notify member(s) of scheduled vehicle assignments or appointments; and
  - Inspect and verify vehicles being turned in for mileage, damage, operational status, cleanliness, and/or issued equipment.

Note: Personnel failing to report with their assigned vehicle and/or issued vehicle equipment shall not be issued a new or replacement vehicle.

Transfers

If members are...	Then members shall...
Transferred or promoted to a function requiring the same vehicle	Retain currently assigned vehicle.
Transferred or promoted to a function requiring an alternate vehicle, i.e., marked, unmarked or specialty vehicle	Contact the Fleet Section for vehicle re-assignment.

Vehicle Disposal

The Fleet Administrator shall:

- Maintain standards and criteria for determining when a vehicle is suitable for disposal;
- Ensure all usable equipment and parts are removed and the vehicle is appropriately prepared for disposal; and
- Provide the Commonwealth of Massachusetts Operational Services Division with the vehicle identification number of disposed vehicles.

Extended Leave

Position	Responsibilities
Member	Shall return the following issued equipment to their Troop/Section/Unit Commander when on extended leave in excess of thirty (30) days: • Assigned vehicle along with issued vehicle equipment; and • Department issued fuel card, transponder and snow gate access cards.
Troop/Section Commander	• Shall notify the Fleet Administrator when issued vehicles and equipment are returned due to extended leaves; and • Advise the location of the vehicle and equipment.
Fleet Administrator	• Re-assign vehicle based upon the needs of the Department; and • If practicable, members returning to full duty should be re-assigned the same vehicle.

Subject: Vehicle Management	Number: ADM-19

Forfeited/ Donated Vehicles

The Fleet Administrator has the authority to accept or reject vehicles on behalf of the Department.

Any vehicle accepted by the Department, shall be:

- Delivered to the Fleet Section with appropriate documentation (e.g. order of forfeiture, certificate of title);
- Inspected for mechanical and/or physical safety defects prior to acceptance and registration;
- Assigned a Fleet vehicle computer number; and
- Assigned by the Fleet Administrator based on the needs of the Department.

References: ADM-19A Vehicle Use and Maintenance;
MPAC 41.1.3.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**ADM-19A**
Subject:	
Vehicle Use and Maintenance	

Policy

Department vehicles shall be maintained in a safe, clean and serviceable condition for reasons of safety, operational readiness, and to enhance the Department's public image. For the purposes of this policy, members shall include sworn and civilian employees of the Department.

Members assigned vehicles belonging to other authorities or governmental agencies shall adhere to the vehicle use and maintenance policies of those particular authorities/agencies.

Required Equipment

Vehicles used for patrol purposes shall be equipped with, at a minimum, the following:

- Emergency lights and siren;
- Medical kit;
- Fire extinguisher;
- Radios;
- Detainee safety barrier (marked, semi marked, low profile vehicles);
- Conspicuous markings (marked, semi marked vehicles, low profile vehicles), including, but not limited to reflective chevrons/pinstriping configured as determined by the Fleet Administrator; and
- All other equipment issued with, or made part of the vehicle according to Department specifications.

Vehicle Inspection

Vehicles and equipment shall be inspected:

- At the beginning of each shift by the vehicle operator;
- For damage, contraband, and/or evidence before and after transporting detainees;
- Quarterly by Station/Unit Commanders and documented according to Department procedures;
- In preparation for line or staff inspections; and
- Upon request by the Fleet Administrator.

Equipment in need of replacement/replenishment shall be coordinated through the member's Station/Section/Unit Commander.

The member shall immediately report, in writing, to their immediate supervisor and the Fleet Administrator, any damage or vandalism to Department vehicles.

Any damage to a Department vehicle caused by a person arrested, detained, transported to court or other non-Department employee shall be immediately reported to the Fleet Section in order to collect restitution. The Fleet Coordinator shall make arrangements for repairs through the Fleet Section.

Installation of Non-Issued Equipment, Adding or Removing Window Tint or Vehicle Alteration

Members shall not install non-issued equipment and/or add or remove window tint in any Department vehicle without prior written authorization from the Fleet Administrator.

Issued Department vehicle equipment shall not be altered without prior written authorization from the Fleet Administrator.

Members requesting to install non-issued equipment and/or add or remove window tint in Department vehicles shall:

- Make written requests through the appropriate channels to the Troop/Section/Unit Commander;
- Agree in writing to assume all responsibility for the loss or theft of the equipment, and any damage caused to the vehicle associated with the installation or removal of the equipment;
- Assume all costs associated with the purchase, installation, and service and/or maintenance fees associated with the installed equipment;
- Notify the Fleet Administrator of the location where the professional installation of the equipment shall occur; and
- Immediately remove any equipment as directed by the Fleet Administrator or proper authority.

The Troop/Section/Unit Commander shall review all requests and forward approved requests to the Fleet Administrator or the proper authority.

The Fleet Administrator shall:

- Approve or deny all written requests; and
- Forward the written approval or denial to the appropriate Troop/Section Commander.

Installation of Non-Issued Equipment, Adding or Removing Window Tint or Vehicle Alteration, continued

Vehicle Ornamentation

Members shall not affix/install vehicle ornamentation on or in any Department vehicle, including vehicles assigned to various authorities or other governmental agencies, unless approved in advance, and in writing, by the Deputy Superintendent and the Fleet Administrator.

Vehicle Alteration

Members shall not:

- Remove, cover, or obscure the display of the issued registration plates; or
- Remove cruiser markings from Department vehicles without prior authorization from the Fleet Administrator or proper authority.

Recalls

Recalls issued by the Department or the manufacturer regarding Department vehicles shall be posted by the Fleet Administrator according to Department procedures.

Members who are assigned Department vehicles shall upon notification of a recall:

- Contact an authorized service facility to schedule an appointment for service;
- Ensure the recall work is completed as ordered;
- Forward the repair order to the Fleet Section; and
- Retain a copy of the repair order.

Vehicle Use

Members shall operate Department vehicles in a cautious manner, and in conformance with Department Policies and Procedures, Rules and Regulations, and applicable Massachusetts General Laws.

Department vehicles shall be used for:

- Official use only;
- Commuting to and from home to assigned work location;
- Scheduled work assignments, callouts, or training; and
- Paid Details (undercover vehicles shall not be used at road construction sites.)

Members who use a Department vehicle shall:

- Notify their supervisor and receive authorization prior to using the vehicle outside of normal scheduled work hours, scheduled work assignments, callouts, training, details, or when on any type of time off or days off.

Vehicle Use, continued

Supervisors shall:

- Only authorize a member to use a Department vehicle when the member is on time off or days off for official Department business; and
- Be responsible for documenting each request and authorization.

Maintenance

The operators of Department vehicles shall be responsible for:

- Maintaining a clean exterior and interior;
- Scheduling routine service and repairs with Fleet Section personnel, or at authorized service facilities;
- Reporting all malfunctions in Department vehicles to the Fleet Administrator;
- Ensuring the vehicle registration is current;
- Ensuring the state safety and emission inspection is current;
- Submitting monthly cruiser information according to Department procedures;
- Daily inspection checks; and
- The removal of snow and ice.

Daily Inspection Checks

- All Department Members shall ensure that their assigned vehicle is in proper working order.

Scheduled Maintenance

All Department Members are required:

- To have their currently assigned Department vehicle routinely serviced; and
- To have an oil change at a Department Fleet Facility every 9,000 miles or six (6) months, whichever occurs first.

Appointments shall be made with each individual Fleet Facility prior to mileage/month deadline. No member shall:

- Have their cruiser serviced at a third party commercial service facility, unless the service is specifically pre-approved by the Fleet Administrator.

Troop/Station/Section/Unit Commanders that have specialty, spare, and/or pool vehicles assigned under their command shall ensure compliance.

Fuel Cards

Fuel cards issued to Department members are restricted to the purchase of fuel for assigned Department vehicles. All purchases for items, other than fuel, shall result in the payment of restitution and/or disciplinary action. Members utilizing fuel cards shall:

- Sign a receipt when issued a fuel card;
- Enter Fleet vehicle computer number for PIN and current mileage when fueling;
- Immediately report lost or stolen cards in writing to the Fleet Section, through channels;
- Fuel vehicles at authorized facilities;
- Purchase regular unleaded fuel only, unless otherwise authorized;
- Use self-service facilities, whenever possible, to assist in controlling Department fuel expenditures;
- Ensure vehicle fuel tanks remain at least half full at all times; and
- Turn in fuel cards through channels to the Fleet Administrator upon any leave in excess of thirty (30) or more days.

Note: Members shall not leave their vehicles running while unattended, unless within the scope of their duties (e.g. motor vehicle stops pursuant to M.G.L. c. 90, § 13).

Transponders and Snow Gate Access Cards

Non-revenue Fast Lane Transponders and Snow Gate Access Cards shall only:

- Be utilized for official business in Department assigned vehicles within the Commonwealth of Massachusetts.

Members traveling outside of the Commonwealth shall:

- Disable their transponders;
- Pay tolls personally; and
- File for reimbursement through the standard member expense reimbursement process.

Electronic data associated with the use of these items shall be monitored to ensure compliance. Use of non-revenue Fast Lane Transponders and Snow Gate Access Cards constitutes express consent for the Department to monitor and/or inspect any data created in the course of such use.

Members assigned non-revenue Fast Lane Transponders and Snow Gate Access Cards shall:

- Use the Fast Lane;
- Disable their transponders when traveling out of state;
- Immediately report lost or stolen transponders or Snow Gate Access Cards in writing to the Fleet Administrator, through channels; and
- Turn in non-revenue transponders and Snow Gate Access Cards through channels to the Fleet Administrator upon any leave in excess of thirty (30) or more days.

Specialty Vehicles

Operation of Specialty Vehicles assigned to Specialized Sections/Units shall adhere to the following:

- Use of Specialty Vehicles shall be dictated by circumstances requiring their deployment/use and shall be authorized by the Section/Unit Commander(s);
- Operated by trained, qualified and duly licensed operators assigned to the Section/Unit as approved by the Section/Unit Commander;
- Section/Unit Commander(s) shall ensure that proper training for members assigned is provided for the Specialty Vehicle(s) to be operated;
- Section/Unit Commander(s) shall maintain a file containing all training records and training certifications for their members operating Specialty Vehicle(s);
- Section/Unit Commander(s) shall assign one designee to be responsible for proper maintenance and related equipment associated with the Specialty Vehicle(s) assigned to the Section/Unit. All maintenance will be coordinated with the Fleet Section;
- Section/Unit Commander(s) will maintain updated Operating Manuals for the assigned Specialty Vehicle(s); and
- Section/Unit Commander(s) will determine the equipment to be maintained on assigned Specialty Vehicle(s), if any, and will maintain a record of said equipment and coordinate replacement/replenishment of specialized equipment.

Emergency Operation and Response

Members responding in emergency vehicles shall operate vehicles with due care and regard for the safety of all persons and property.

Members, in an emergency and while in the performance of duty:

- May drive in excess of the applicable speed limit, if exercising caution and due regard under the circumstances;
- May drive through an intersection, contrary to traffic signs or signals, **after coming to a full stop**, and then proceeding with caution; and
- **Shall never pass** a school bus with red lamps flashing that has stopped to allow pupils to alight or board.

Emergency Operation and Response, continued

Response	Action
Non-emergency/non-life threatening.	• Emergency lights and/or siren need not be used; and • Observe all traffic laws and regulations.
Emergency, but non-life threatening.	• Emergency lights and sirens may be utilized; and • May use discretion in approach.
Actual or potential life-threatening injuries or violent situations.	• Utilize emergency lights and sirens; • Expeditious response with due care and regard for public safety; and • May use discretion in approach.

Seatbelts

All occupants shall properly wear seatbelts while traveling in any state owned vehicles as mandated by Executive Order No. 241.

Airbags

No object shall be placed on or in the path of airbags for safety reasons. Airbag switches shall not be installed in any Department vehicle without the prior written approval of the Fleet Administrator.

References:
ADM-19 Vehicle Management;
TRF-20 Department Vehicle Crashes;
Executive Order No. 241 Use Of Seat Belts By State Employees;
MGL c. 89, § 7B;
MGL c. 90, § 13;
MGL c. 90, § 14;
MPAC: 41.1.3, 41.2.1, 41.3.2, 41.3.3.

Promulgated By: John E. Mawn, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**ADM-19B**
Subject:	
Automated Vehicle Locator (AVL) Technology	

Policy

The purpose of this policy is to establish guidelines and procedures for the use of the Department's Automated Vehicle Locator (AVL) Technology. AVL is designed to increase officer safety and accountability by enhancing the ability to rapidly locate and deploy Department personnel and resources. AVL technology also improves coordination and resource management during tactical situations, assists in improving response times to radio calls, and increases situational awareness for all employees.

The Department's AVL utilizes global positioning system (GPS) to determine the location of Department personnel and resources.

AVL technology allows for real-time command and control of Department resources. Knowledge of resources that are in the vicinity of an incident improves officer safety, increases operational efficiency, and provides the Department with a more efficient and dependable means of enforcing work rules. Accordingly, it is the Department's goal and policy to utilize AVL in all marked Department cruisers and as many additional vehicles and resources, subject to operational demands and funding, as determined by the Colonel.

Safety and accountability are the primary goals of the AVL system; however, AVL data shall be used for all relevant purposes including but not limited to, the deployment of personnel, operational efficiency, patrol strategy, personnel and other investigations, the enforcement of work rules, regulations, policies, customs, practices, procedures, orders, commands, and/or directives.

Department employees are reminded that, in relation to the Department's receipt and use of AVL data, they have no expectation of personal privacy.

Subject	Number
Automated Vehicle Locator (AVL) Technology	**ADM-19B**

Definitions

Automated Vehicle Locator Technology (AVL): An electronic means for automatically determining and transmitting the geographic location of Department resources to include: personnel, vehicles and crafts. Examples of AVL technology include, but are not limited to: GPS equipped radios, cellular devices, Mobile Data Terminals (MDTs), and stand-alone hardware devices.

Global Positioning System (GPS): A satellite system that provides geo-coordinates and time information to a GPS receiver.

On Duty: For the purposes of this Order only, shall refer to any period of time that an employee of the Department is performing any Department function or using a Department vehicle or resource, to include, but not be limited to, the following: the performance of duties, whether assigned or self-initiated, uniformed or plain clothed, patrol, investigative and administrative functions, reporting and traveling to and from work assignment, court, paid detail or training, and/or commuting to and from home.

Administration

All on duty Department personnel issued AVL Technology, or a vehicle or resource equipped with AVL, shall use AVL in accordance with all of the following:

- Unless expressly exempted by the Colonel or his/her designee, all on duty members equipped with AVL Technology shall, except where AVL is not self-activated, activate AVL systems or devices at the beginning of being on duty and shall keep it activated until off duty. This requirement includes activating GPS equipped portable radios, logging on to GPS equipped MDT, and activating assigned cellular devices and/or modems.

- A member shall report technical problems and or malfunctions relating to the operation of the AVL system immediately to their supervisor and to the Communications Section. The malfunction shall be recorded in the Daily Administrative Journal (DAJ) by the member. This entry shall include who the malfunction was reported to.

- Any member operating a Department vehicle or resource with a malfunctioning AVL system shall comply with the Officer/Vehicle Status notifications required by ADM-21 Communications.

- Supervisors and the Communications Section shall immediately report any malfunction of the AVL system to the Executive Office of Technology Services and Security (EOTTS).

- At least once during a shift, Troop/Section/Unit Commanders, or designees, shall determine the AVL systems of each on duty member, under their command, are working properly.

Subject	Number
Automated Vehicle Locator (AVL) Technology	**ADM-19B**

Equipment

- No member shall use or install any equipment or items that may interfere with Department authorized AVL equipment.
- Members shall not tamper with the AVL/GPS receiver, antenna, wiring, and/or software or attempt to hinder the systems designed performance. Any misuse, abuse, alteration or modification of the AVL software, hardware or any associated components or any violation of this General Order may result in disciplinary action.

Exemptions

The Colonel shall determine which vehicles and resources shall be equipped with AVL technology. A Division Commander, or designee, may authorize the temporary disabling of AVL equipment for members or resources under their command, and shall, when authorized, document the reasons for same in writing.

- Any member whose assignment would be adversely affected by having location information recorded/published may request authorization from the member's Division Commander, or designee, to temporarily disable the AVL system for as long as necessary to complete the assignment.

AVL Records

AVL data:

- Shall be the property of the Department of State Police;
- Shall not be disseminated without authorization from the Department;
- Shall not be accessed, copied, or released for non-law enforcement purposes except as authorized in this policy or as required by law;
- Shall be preserved and/or made available in compliance with all legal obligations and orders, for investigative and training purposes and other needs of the Department;
- Shall be securely stored and disposed of in accordance with state records retention laws; questions related to storage and disposal shall be directed to the Department's Legal Section.; and
- May be preserved at the request of a Division Commander or designee or for any lawful reason.

Accessing AVL Data

Members and employees may only access Department AVL data when they are expressly authorized to access such data in the course of their assigned duties and in accordance with SPAM Unit 5A-Commonwealth CBA.
Other requests for access to AVL data, live or stored, shall be made in writing and forwarded through channels to the member/employee's Division Commander or designee.

Subject	Number
Automated Vehicle Locator (AVL) Technology	**ADM-19B**

Audits

The Colonel/Superintendent or designee may authorize audits of any AVL device to ensure system integrity and functionality.

The Colonel, Deputy Superintendent, Division Commanders and/or their designee(s) shall have access to AVL data for any lawful, relevant purpose, including but not limited to situational awareness, response times, analysis and improvement of patrol tactics, improvement of officer safety, criminal or personnel investigations, and the enforcement of existing work rules, regulations, policies, customs, practices, procedures, orders, commands, and/or directives.

References

ADM-21 Communications;
SPAM Unit 5A-Commonwealth CBA, Comm-SPAM Executed on the Record 2018-2020 12-2-19.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**ADM-20**
Subject:	
Weapons Management	

Policy

The Armorer shall provide oversight for the control and operational readiness of all Department weapons and ammunition, from acquisition to final disposition.

Members shall continually inspect all weapons and ammunition issued to them or under their control, to ensure cleanliness and operational readiness.

Definition

Armorer: A member designated by the Colonel/Superintendent, responsible for all weapons and ammunition under their control or in storage at the Armory.

Firearms: All firearms, rifles, shotguns, and machine guns issued by the Department.

Armorer

The Armorer shall:

- Maintain an accurate inventory of all weapons;
- Maintain all SP 9 Record of Issue and SP 255 Equipment Transfer/Disposition forms;
- Update the Department Soft Body Armor/Weapons Inspection database;
- Maintain an inventory of ammunition and firearms related supplies;
- Ensure that sufficient quantities of ammunition, parts, and supplies remain at the Armory for Department use;
- Coordinate all firearms repairs;
- Conduct training for all members;
- Ensure each Station/Section/Unit has a suitable bullet trap or body armor for use in unloading firearms; and
- Be available to provide temporary replacement firearms.

Firearms Issue or Transfer

Each firearm issuance and transfer shall be recorded on the SP 9. The Armorer shall ensure the correct information is updated on PayStation.

Commanding Officers that have firearms assigned to the Station/Section/Unit shall complete a SP 255 form indicating:

- Description of firearms including serial number; and
- Date and location of assignment.

Commanding Officers shall forward one (1) copy to the Armorer and retain a copy for the Station/Section/Unit records.

Storage of Firearms and Ammunition

Commanding Officers that have firearms assigned to their Station/Section/Unit shall:

- Provide a secure, locked, and alarmed storage area;
- Keep all stored items in a state of operational readiness and available for emergency use at any time; and
- Permit immediate accessibility only to authorized members.

Seizure of Firearms

Upon seizure of a duty firearm, the supervisor shall contact the Armorer to:

- Determine if the member has additional issued firearms; and
- Coordinate storage of the seized duty firearms(s).

Disposal of Weapons

Upon determination that Department firearms or ammunition have become obsolete or inoperable, the Armorer shall complete a SP 255 indicating:

- Description of item;
- Reason and method of disposal (sale, trade-in, destruction); and
- Name of receiving agency/company and signature of receiving party.

The Armorer shall dispose of the item in accordance with the guidelines established by the Commonwealth of Massachusetts.

Inspections

During range qualification all firearms shall be inspected for condition and operational readiness by the Armorer or designee.

Supervisors shall ensure:

- A firearms inspection has been completed quarterly for all subordinates during the months of January, April, July, and October;
- A report of the inspection is documented on PayStation; and
- Members on leave during the quarterly period have their firearms inspected on the first day that the member returns to duty.

Only members trained in the inspection of specific firearms shall inspect that particular type of firearm.

Inspections, continued

Members submitting a firearm for inspection shall:

- Ensure that the firearm is in a safe and unloaded condition with the magazine removed;
- Present the firearm with the slide locked in the open position;
- Shotguns shall be presented for inspection with the action in the open position; and
- Rifles, machine guns and submachine guns shall be presented for inspection in a safe manner as directed by the Inspector.

Weapons shall be unloaded in a safe manner consistent with training, using a suitable bullet trap or ballistic vest as a backdrop in a safe area approved by the Armorer.

Inspectors Duties

Only members trained in the inspection of specific firearms shall inspect that particular type of firearm. Inspectors may use a SP 608 Weapons Inspection form as a guideline during the inspection process.

Firearms Inspectors shall:

- Inspect all Department firearms as assigned and document on the Department database during the months of January, April, July, and October;
- Detail all inadequacies on the database; and
- Remove any weapon or ammunition found to be defective and forward to the Armorer for repair or replacement.

Temporary Firearms

Commanding Officers shall:

- Ensure that the member with the defective firearm is issued a temporary replacement firearm by the Armorer; and
- Document the issue of the temporary firearm on a SP 9.

The Armorer or designee shall issue temporary firearms. The Armorer may be contacted through the GHQ Communications Section.

Leave

Commanding Officers of a member who is on any leave in excess of thirty (30) days shall contact the Armorer for storage of Department issued firearms and ammunition.

References:

SP 9 Record of Issue Form;
SP 255 Equipment Transfer/Disposition Form;
SP 608 Weapons Inspection Form;
UOF-04 Use of Force Equipment.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**ADM-21**
Subject:	
Communications	

Policy

The Department shall maintain an effective and efficient communications system to aid in the performance of its public safety mission.

The Department shall ensure continuous communication accessibility through a mission-critical, multi-channel radio system capable of two-way operation on joint public safety frequencies.

Troop Duty Officers, Desk Officers and Dispatchers shall utilize available technologies, as applicable, including but not limited to: radio, CAD (Computer Aided Dispatch), Department issued technology, and Automated Vehicle Locator (AVL) to determine which members are available for service and to maintain communication with members.

The Department shall comply with all Federal Communications Commission (FCC) procedures and requirements.

Within the content of this policy, members shall refer to sworn Department members and employees shall refer to civilian Department members.

Positions and Responsibilities

Position	Duties
Colonel/Superintendent or designee member(s)	• Designate personnel to Communications Staff positions.
Director of Telecommunications	• Supervise all personnel assigned to the Communications Section; • Serve as "Keeper of the Records" for the Communications Section; • Oversee the administration of the audio recordings of Department radio frequencies; and • Oversee the recording, retention and preservation of 9-1-1 call payload and Department radio payload as outlined in this policy.
Communications Officer (Commissioned Officer)	• Supervise sworn members assigned to the Communications Section; and • Serve as the DCJIS Administrator and Point of Contact for the Department.

Positions and Responsibilities, continued

Position	Duties
Director of Dispatch Services	• Supervise all civilian personnel in the Dispatch Services Unit.
Radio System Manager	• Supervise all civilian personnel in the Radio Unit; and • Provide technical expertise in the operation and implementation of Department radio systems.

Recording & Data Retention

The Department shall maintain immediate playback capability of recorded telephone and radio communications.

Requests for immediate playback of 9-1-1 and/or radio communications shall be directed to the Troop Dispatcher of jurisdiction.

9-1-1 Payload

The Department shall record all incoming/outgoing 9-1-1 payloads (audio, text, photo, video, telematics, etc.) at all of its Public Safety Answering Points (PSAPs). 9-1-1 payloads shall be retained and preserved for a minimum period of one (1) year. Records shall be secured and accessible only to authorized personnel.

9-1-1 Call Detail Records

The Department shall capture all 9-1-1 call detail records at all of its PSAPs. 9-1-1 call detail records shall be retained and preserved for a minimum period of three (3) years. Records shall be secured and accessible only to authorized personnel.

Radio Payload

The Department shall record/capture all operational radio payload (audio, metadata, etc.), as determined by the Colonel/Superintendent or designee. Radio payloads shall be retained and preserved for a minimum period of one (1) year. Records shall be secured and accessible only to authorized personnel.

Audio Recordings

Requests for cellular and radio audio recordings shall comply with all legal requirements and shall be provided for the needs/requests of the Department including, but not limited to, investigations, training, court-orders, public record requests, or as otherwise directed by the Colonel/Superintendent.

Audio recording requests shall be forwarded utilizing the SP-623 Cellular 911 & Radio Transmission Recording Request Form.

Communication Facilities and Equipment

Access to Department Communications Centers and equipment shall be restricted to authorized personnel.

Communication Facilities and Equipment, continued

Each Department facility is equipped with an alternative power source/generator, sufficient to operate the radio systems and other vital equipment, in the event of a primary power source failure.

The alternative power source shall be:

- Accessible only to authorized personnel;
- Inspected and tested weekly by the Troop/Station/Section Commander or designee who shall document said inspection/test; and
- Maintained at least annually, including documented testing and/or operation at full load.

Emergency Service Numbers

The Troop/Station/Section/Unit Commanders shall ensure:

- Telephone numbers and addresses of available emergency service agencies are up to date and readily available to dispatchers, desk officers, as well as other communications personnel; and
- Tactical dispatching plans or emergency operational plans that may affect facilities within their specific jurisdiction (e.g., prisons, nuclear plants, sports facilities) are current and readily available.

Emergency Radio Alarm Activation

The activation of an emergency radio alarm of a member shall be deemed notification of an "Officer In Trouble" until proven otherwise.

Upon a member activating the emergency alarm the Dispatcher shall immediately:

- Initiate contact with the member;
- Request a "Code 30 Status" and follow Communication Section Emergency Radio Alarm Protocols; then
- Query the AVL database for the member's location.

If able to communicate, the activating member shall broadcast their cruiser number or name, nature of the emergency and exact location.

Upon confirmation of the "Code 30", or if the member does not respond, the barracks Desk Officer shall initiate the response of additional resources, including MSP personnel and local law enforcement, providing the members last known location. Additional technology shall be utilized to identify, and/or verify, the location of the member.

A "Code 1" shall be initiated upon confirmation of the "Code 30" or if the member fails to respond to attempts to communicate with them.

The Troop Duty Officer shall assume responsibility for oversight of the "Code 1" assisting the Dispatcher and barracks Desk Officer with actions related to the "Code 30" response.

The "Code 1" should remain in effect until confirmation of the activating member's status can be verified by the member or responding members.

Emergency Radio Alarm Activation, continued

Inadvertent activation of the emergency alarm shall be immediately addressed by the member. The member shall broadcast "Code 17" in response to the Dispatcher request of "Code 30 Status". The Dispatcher will confirm receipt of the "Code 17" broadcasting the updated status of the activating member.

The member shall reset the inadvertent emergency alarm activation by pressing and holding the emergency button for approximately three (3) seconds until the radio tones indicating clearance of the activation, or turning the radio off and on again.

Radio Decorum

Department members and employees(s) shall ensure:

- Department radio communications/messages have first priority;
- They properly identify themselves and use clear diction when communicating on the Department network;
- Radio transmissions shall be necessary, professional, concise, and formal at all times using a clear spoken message-based on common terminology; and
- When making requests for law enforcement information, they shall do so via their assigned radio frequency, unless doing so would compromise an investigation or a member's safety.

Alternative Reporting Methods

Emerging technologies may result in the receipt of information in a non-traditional manner (e.g.: text, e-mail…) requiring a Department response. Personnel receiving information through non-traditional reporting methods shall:

- Evaluate the need for a Department response;
- Record the details of the information received and Department response in the appropriate CAD/RMS, DAJ, or ACISS call log;
- Assign member(s) to calls requiring a Department response when applicable, or route the information to the appropriate Division/Section/Unit for follow up if applicable;
- The Division /Section/Unit shall assign member(s) to calls requiring a Department response; and
- Communicate the Department response to the reporting party where applicable/appropriate.

Incident Command

The National Incident Management System (NIMS) has integrated existing best practices into a consistent, nationwide approach to domestic incident management at all jurisdictional levels and across functional disciplines.

Department personnel involved with a complex critical incident shall:

- Use a clear spoken message-based on common terminology; and
- Refrain from using codes for radio communications.

Radio Interoperability

In an effort to simplify communications while promoting interoperability, plain English will be utilized in all situations requiring inter-agency operations.

Radio Codes

To eliminate lengthy radio transmissions and maintain confidentiality, the following codes shall be used for all radio broadcasts, whenever practicable:

CODE 1	STANDBY FOR AN EMERGENCY - Cease and desist all unnecessary radio traffic. Only primary dispatchers and officers engaged in the emergency shall transmit messages**.**
CODE 2	TELEPHONE YOUR STATION
CODE 3	TELEPHONE (person) AT (number).
CODE 4	CRUISER OUT OF SERVICE Specify location.
CODE 5	CRUISER NOW IN SERVICE
CODE 6	WHAT IS YOUR LOCATION?
CODE 7	RETURN TO YOUR STATION OR SPECIFIC LOCATION
CODE 8	STOPPING A SUSPICIOUS VEHICLE – Transmit vehicle make, model, color, registration number, number of occupants, and give EXACT LOCATION.
CODE 9	REQUEST LISTING ON-Transmit registration number and/or vehicle identification number of motor vehicle, and give EXACT LOCATION.
CODE 10	REQUEST STOLEN RECORD ON - Transmit registration number and/or vehicle identification number or serial number of suspected stolen property, and give EXACT LOCATION.
CODE 11	REQUEST LICENSE DATA ON - Transmit license number and give EXACT LOCATION. If license number is not known, transmit name and DOB.
CODE 12	ANY MESSAGES FOR ME?
CODE 13	RADIO TEST CALL. Give signal strengths as follows: R-1 Barely audible; R-7 Moderately strong signal; R-3 Weak signal; R-9 Strong signal loud and clear. R-5 Fairly good signal;
CODE 14	MISSING OR WANTED CHECK - Transmit name, race, sex, DOB, social security number, registration of vehicle if applicable, and give EXACT LOCATION.
CODE 15	OFFICER REQUESTING ASSISTANCE - Transmit EXACT LOCATION and, if able, reason for request.
CODE 16	CRASH INVESTIGATION (state type) AT (location)
CODE 17	CLEAR – From a previous assignment completed and now back on patrol and/or original assignment and available.
CODE 18	PERMISSION TO LEAVE ASSIGNED PATROL - Transmit EXACT LOCATION, reason and estimated time of absence.
CODE 20	INVESTIGATION (state type) AT (location)
CODE 22	CELLULAR CALLER ADVISEMENT/NOTIFICATION
CODE 30	**OFFICER IN TROUBLE/ TRANSMIT EXACT LOCATION**

Phonetic Alphabet

Members shall utilize the following phonetic alphabet.

A	Alpha	**N**	November
B	Bravo	**O**	Oscar
C	Charlie	**P**	Papa
D	Delta	**Q**	Quebec
E	Echo	**R**	Romeo
F	Foxtrot	**S**	Sierra
G	Golf	**T**	Tango
H	Hotel	**U**	Uniform
I	India	**V**	Victor
J	Juliet	**W**	Whiskey
K	Kilo	**X**	X-ray
L	Lima	**Y**	Yankee
M	Mike	**Z**	Zulu

References:
National Incident Management System (NIMS) October 2017;
MGL Chapter 6A;
CMR 560 § 2;
CMR 560 § 3;
SP 623 Cellular 911 & Radio Transmission Recording Request;
MPAC 81.2.2, 81.2.4, 81.2.5, 81.2.8, 81.3.2, 82.2.5.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

1708

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**ADM-22**
Subject:	
Court Attendance and Fees	

Policy

Department employees shall comply with all court orders and summons.

Employees shall be compensated for court attendance according to their applicable collective bargaining agreements.

Definitions

Court Officers: Shall be designated by a Troop Commander as the Officer-in-Charge of Instruments for Breath Alcohol Testing and be the Keeper of Records for their jurisdiction's Breath Alcohol Testing Devices.

Day Off: Any regularly scheduled day off, including a holiday or an administrative day off.

Nighttime Shift: A regular duty assignment to the evening or midnight shift.

Vacation Day: A paid vacation day within an approved scheduled vacation week.

Documentation

All court appearances, depositions, or consultations shall be accurately documented by appropriate log entries in the Daily Administrative Journal (DAJ) including the following:

- Case name;
- Type of appearance;
- Time in/out; and
- Court location.

All court entries within the DAJ shall be reviewed daily by the Station/Unit Commander or designee.

Payment for Court Appearances

Members may be entitled to payment of a court fee for attendance at a state or federal court if the member is on duty at night, on vacation or furlough, or on a regularly scheduled day off and is a:

- Witness testifying in court on behalf of the Commonwealth or United States;
- Subpoenaed witness in criminal court testifying in an official capacity; or
- Defendant in court in a civil rights case in which the member was acting in an official capacity within the scope of employment.

Members may not receive a court fee or additional pay when:

- They are not a witness for the Commonwealth;
- They are the plaintiff in a case; or
- They are a witness, on behalf of another Department member, not acting in an official capacity.

Note: Except when on an approved scheduled vacation week, no member shall be granted paid time off which conflicts with a scheduled court appearance, or would result in overtime being generated for the court appearance.

Witness Fees

Any member entitled to a court witness fee may receive and accept such fee, in lieu of but not in addition to, any other type of compensation (MGL c.262, §50.)

Members shall not receive a court witness fee when:

- Any other type of compensation is received during the period of time of court appearance;
- Appearing at a second court during a time for which the member is still receiving compensation for their appearance at the first court attended;
- Working a day shift;
- On sick, injured, or extended leaves; or
- They are not a witness for the Commonwealth.

Travel Fees

Members may be entitled to a travel allowance from the court when:

- A private vehicle is used to travel to and from court held in a city or town other than a city or town in which the member resides.

Note: Travel allowance is only authorized from the actual point of origin and actual point of return from court attendance.

Travel Fees, continued

Members are not entitled to any travel allowance if:

- A state-owned vehicle is used;
- Receiving mileage allowance from any other government or private source; or
- Duplication of mileage occurs from more than one (1) court within one (1) day.

Court Fees

Court appearance fees shall:

- Be computed from the start of the appearance, or the member's actual arrival time, whichever is later, until the end of the appearance;
- Be consistent with Massachusetts General Laws and collective bargaining agreements, unless it overlaps with a member's other duties; and
- Not be paid for member's travel time to or from court.

Injured Leave Status

Members on injured leave subpoenaed to appear in court shall:

- Notify their immediate supervisor and the Court Officer who issued the SP 189 Court Appearance Notification;
- Request a continuance or reschedule the appearance through the court officer of jurisdiction; or
- If a continuance is not granted, request authorization to appear from the Troop/Section Commander or designee.

Temporary Modified Duty Status

Members on Temporary Modified Duty notified to appear in court shall:

- Notify their immediate supervisor and the Court Officer who issued the SP 189;
- Request a continuance or reschedule the appearance; or
- If a continuance is not granted, request authorization to appear from the Troop/Section Commander or designee.

Extended Leave Status

Members on extended leave subpoenaed to appear in court shall:

- Notify their immediate supervisor and the Court Officer who issued the SP 189;
- Request a continuance or reschedule the appearance through the court officer of jurisdiction; and
- Not appear in court on behalf of the Department.

Court Responsibilities

Position	Responsibilities
Employees	• Check the Department email system every work shift, to remain apprised of newly assigned court cases or status changes to pending cases; • Print any emailed SP 189 Court Card Notifications; • Submit complaint applications to the Court Officer of jurisdiction; • If a summons is received directly from an authorized agent of the court, immediately submit the hard copy to the Court Officer of jurisdiction and request a SP 189; • Have any SP 189's signed by the required parties, if any overtime hours are generated by a court appearance; • The SP 189 shall be date/time stamped by the Clerk's Office at the conclusion of the case, if more than four (4) hours of overtime are generated by any court appearance on any single calendar day; • Have the Assistant District Attorney sign the SP 189, including the actual time of the member's appearance, if a date/time stamp is not available; • Notify the Court Officer of jurisdiction of any continuances and the parties who requested the continuance; and • Enter information on the case disposition, sign, and submit the SP 189 to their assigned Station/Section /Unit.
Court Officer	• Schedule employee's court appearances in an effort to minimize overtime; • Immediately enter information from summonses, continuances, or cancellations into the Department court database; • Issue the SP 189 for proceedings not scheduled by other Court Officers (e.g., Grand Jury, Superior Court, Federal Court, depositions); • Immediately advise affected employees of court case assignment and status changes to pending cases using all available methods; • Advise the Station/Unit Commander of any court case requiring the appearance of three (3) or more members; • Enter all disposition information into the Department court database;

Court Responsibilities, continued

Position	Responsibilities
Court Officer	• Shall be the Officer-in-Charge of Instruments for Breath Testing Devices according to TRF-14 Operating Under the Influence, and function as the Keeper of the Records; • Provide the Commanding Officer with a weekly list of court notifications; and • Immediately notify their Commanding Officer if a member: o Fails to appear for a scheduled court date; or o Appears at court without prior notification by a Court Officer; or o Is notified to return to court for additional information required by the court during an arraignment.
Commanding Officers	• Review and reconcile all submitted SP 189's prior to approving PayStation court overtime submissions; • Deny any court overtime submitted on PayStation without a proper and signed SP 189; • Retain all submitted Station/Unit court appearance notification forms for inspection for three (3) years; Review requests for court appearances involving three (3) or more members as notified by the Court Officer and consult with the appropriate court authority to determine if any members appearance is not critical to the case; and • Notify the Troop/Section Commander or designee immediately if a member: o Fails to appear for a scheduled court date; or o Appears at court without prior notification by a Court Officer; or o Is notified to return to court for additional information required by the court during an arraignment.
Troop Cases and Report Officers	• Conduct examinations of submitted PayStation and SP 189's for signs of inefficiency or abuse; • Maintain staff supervision of the Court Officers and conduct semi-annual staff inspections of Court Officer's files; • Report inspection findings and analysis to the Troop Commander; and • Assist Court Officers in addressing problems at their assigned courts, or with conflicts between the courts and the Department.

Subject: Court Attendance and Fees	Number: ADM-22

Court Responsibilities, continued

Position	Responsibilities
Troop/ Section Commanders or Designee	• Contact the appropriate court authority to confirm the necessity of the appearance of three (3) or more members on the same day; and • Conduct examinations of submitted PayStation and SP 189's for signs of inefficiency or abuse.

Non-Field Sections/Units

Commanding Officers shall create court appearance guidelines appropriate for their Section/Unit and file a copy with the appropriate Division Commander.

References:

ADM-11E Extended Leaves;
TRF-14 Operating Under the Influence;
SP 189 Court Appearance Notification;
MGL c.262, §50;
MGL c.262, s. 53B, 53C;
SPAM Collective Bargaining Agreement Article 27.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**ADM-24**
Subject:	
Department Radio Call Signs	

Policy

The Department shall promote officer safety and efficiency using a standardized Radio Call Sign procedure.

Standardized Radio Call Signs, as referenced within this General Order, shall be used by all employees for all radio transmissions.

Protocol

Whenever a member requests information over the radio, such requests shall be preceded by, or ended with, the member's exact location.

All transmissions shall be conducted in a concise manner and in accordance with the formats indicated in this General Order. At the end of all transmissions, the receiving party shall acknowledge receipt of the transmission by saying "Received."

Call Sign Structure

The Department shall use the following categories for Radio Call Signs:

- The Executive Branch;
- The Executive Office of Public Safety and Security (EOPSS);
- The State Police Command Staff;
- Division Call Signs;
- Station Identifiers; and
- Specialty Vehicles.

Radio Call Sign Database

The Fleet Administrator shall:

- Maintain a database of assigned cruiser numbers, matching each cruiser number to a vehicle and employee;
- Ensure Radio Call Signs assigned to Executive Branch, EOPSS, and Department Command Staff are included within the database; and
- Not be responsible for, nor maintain a database of call signs outside of the actual vehicle to member assignment.

Department Radio Call Signs

Department employees (sworn and civilian personnel), unless specifically identified within this General Order, shall:

- Use the Fleet Designated Cruiser Number assigned by the Fleet Administrator as their Radio Call Sign.

Employees assigned spare cruisers or pool vehicles shall:

- Use the assigned spare cruiser/pool vehicle's designated cruiser number as their Radio Call Sign; and
- Provide their name, Department ID number, and rank (if applicable).

Call Signs for the Executive Branch, EOPSS and Command Staff

The Department shall assign Radio Call Signs for the Executive Branch, EOPSS, and Department Command Staff. The following Radio Call Signs shall be assigned:

Entity	Call Sign	Assignment
Executive Branch	S-1	Governor
Executive Branch	S-2	Lt. Governor
EOPPS	S-3	Secretary of Public Safety and Security
EOPPS	S4-10	Available for EOPPS
Department Command Staff	1	Colonel/Superintendent
Department Command Staff	2	Lt. Colonel / Deputy Superintendent
Department Command Staff	3	Lt. Colonel / Field Services
Department Command Staff	4	Lt. Colonel / Investigative Services
Department Command Staff	5	Lt. Colonel / Standards and Training
Department Command Staff	6	Lt. Colonel / Homeland Security and Preparedness
Department Command Staff	7	Chief Administrative Officer
Department Command Staff	8	Chief Science Officer
Department Command Staff	10	Chief of Staff for the Colonel/Superintendent
Department Command Staff	11-19	Majors – Division of Field Services (DFS), Non-Troop
Department Command Staff	20-29	Majors and Detective Captains – Division of Investigative Services (DIS)
Department Command Staff	30-39	Majors – Division of Standards and Training (DST)
Department Command Staff	40-49	Majors and Detective Captains – Division of Homeland Security and Preparedness (DHS)
Department Command Staff	50-59	Majors – Division of Administrative Services (DAS)

Department Command Staff	60-69	Majors and Detective Captains Forensic Services Division (FSD)

Division of Field Services

The Division of Field Services shall adhere to the following protocol:

Troop Headquarters shall use the appropriate troop phonetic identifier preceded by the word “Station” as the radio call sign (e.g., "Station H to 756").

Sub-Stations shall use the appropriate phonetic identifier followed by the assigned numerical designation (e.g., "B-1", "D-2"). Troops and Sub-Stations along with their corresponding phonetic identifiers are listed below in the “**Troop and Sub-Station Call-Sign**” table.

Specialty vehicles shall be identified through Radio Call Signs as the name of the unit followed by the assigned number of the vehicle (e.g., “Cycle 5”).

All DFS personnel shall utilize their Fleet Designated Cruiser Number as their Radio Call Sign, except as follows:

Troop Commander:
- Number one (1) attached to the phonetic troop identifier (e.g., "1A”).

Troop Executive Officer:
- Number two (2) attached to the phonetic troop identifier (e.g., "2A”).

Troop Captains:
- Numbers three (3) through five (5) attached to the phonetic troop identifier, (e.g., "3A," "4A," or "5A”).

Operations Officers:
- Numbers six (6) through eight (8) attached to the phonetic troop identifier, e.g., "6A," "7A," or "8A”).

Station Commanders:
- In numeric sequential order, beginning with the number 11 attached to the phonetic troop identifier (e.g., “11A” for the Station Commander of A-1 and “15A” for the Station Commander of A-5);

Division of Field Services, continued

Special Operations Troop "S" Commanders shall be identified as:

- Special Operations Captains (2-4) (e.g., "2S," or "3S," etc.);
- STOP Team Commander- "5S;"
- SERT Commander- "6S;"
- CVES Commander- "1T;" and
- Canine Unit Commander- "1K."

DFS members specified above shall follow their call sign with their rank/name during their initial communication with a Troop Dispatch or Barracks.

Personnel assigned to Troop F, the Commercial Vehicle Enforcement Section, and the Canine Unit, shall use:

- Their assigned Authority cruiser number or their Fleet Designated Cruiser Number as their Radio Call Sign, followed by the phonetic identifier "F," "T," or "K" respectively, (e.g., "121F," "221T," or "437K").

Troop and Sub-Station Call Signs

AHQ – Danvers

- A-1 Andover
- A-2 Newbury
- A-3 Concord
- A-4 Medford
- A-5 Revere
- A-6 Danvers (sub-station)

BHQ – Northampton

- B-1 Lee
- B-2 Shelburne Falls
- B-3 Springfield
- B-4 Cheshire
- B-5 Russell
- B-6 Northampton (sub-station)
- B-7 Shelburne Falls (dispatch)
- B-8 Westfield

CHQ – Holden

- C-1 Athol
- C-2 Millbury
- C-3 Brookfield
- C-4 Leominster
- C-5 Sturbridge
- C-6 Holden (sub-station)
- C-7 Belchertown
- C-8 New Braintree (dispatch**)**
- C-9 Devens
- C-10 Charlton

Troop and Sub-Station Call Signs, continued

DHQ – Middleboro
- D-1 Norwell
- D-2 Yarmouth
- D-3 Dartmouth
- D-4 Middleboro (sub-station)
- D-5 Oak Bluffs
- D-6 Nantucket
- D-7 Bourne

FHQ – Logan Airport
GHQ – General Headquarters-Framingham
HHQ – South Boston
- H-1 Government Center
- H-2 Framingham
- H-3 Foxboro
- H-4 Boston
- H-6 South Boston (sub-station)
- H-7 Milton
- H-8 Weston
- H-9 Tunnels

Division of Investigative Services

Radio Call Signs for Section/Unit members within the Division of Investigative Services, who make radio transmissions over the Troop Radio System, shall:
- Use plain language one word unit name followed by their assigned Fleet Designated Cruiser Number (e.g., "Middlesex 1234 to Station A" or "VFAS 4321 to Station H").

Section/Unit Commanders/Executive Officers within DIS shall:
- Be assigned specific Radio Call Signs for their sections and units;
- Use the number "1" for the Commanding Officer preceded by the section/unit name (e.g., "Middlesex 1 to Station A");
- Use the number "2" for the Executive Officer preceded by the section/unit name (e.g., "VFAS 2 to Station H").

The Division Commander, Division Majors, and Detective Captains are designated call signs in accordance with the "Department Command Staff" table on page 2 of this General Order.

Division of Standards and Training

The Division of Standards and Training personnel shall utilize:
- Their Fleet Designated Cruiser Number as their Radio Call Sign.

The Division Commander and Division Major(s) are designated call signs in accordance with the "Department Command Staff" table on page 2 of this General Order.

Division of Homeland Security and Preparedness

Radio Call Signs for Section/Units Members within the Division of Homeland Security and Preparedness, who make radio transmissions over the Troop Radio System, shall:

- Use plain language one word unit name followed by their assigned Fleet Designated Cruiser Number (e.g., "Fraud Id Unit 1234 to Station A").

Section/Unit Commanders/Executive Officers within DHS shall:

- Be assigned specific Radio Call Signs for their sections and units;
- Use the number "1" for the Commanding Officer preceded by the section/unit name (e.g., "Fraud Id Unit 1 to Station A");
- Use the number "2" for the Executive Officer preceded by the section/unit name (e.g., "Fraud Id Unit 2 to Station H").

The only two exceptions to this are as follows:

- The Air Wing Commanding Officer will utilize "Whiskey 1" and the Marine Unit Commanding Officer will utilize "Mike 1"; and
- The Air Wing Executive Officer will utilize "Whiskey 2" and the Marine Unit Executive Officer will utilize "Mike 2".

The Division Commander, Division Majors, and Detective Captains are designated call signs in accordance with the "Department Command Staff" table on page 2 of this General Order.

Division of Administrative Services

The Division of Administrative Services personnel shall utilize

- Their Fleet Designated Cruiser Number as their Radio Call Sign.

The Division Commander and Division Major(s) are designated call signs in accordance with the "Department Command Staff" table on page 2 of this General Order.

Forensic Services Division

The Forensic Services Division personnel shall utilize

- Their Fleet Designated Cruiser Number as their Radio Call Sign.

The Division Commander, Division Major(s) and Detective Captain(s) are designated call signs in accordance with the "Department Command Staff" table on page 2 of this General Order.

GHQ/ COMSEC

The General Headquarters / Communications Section shall be identified with the phonetic letter "G."

Subject: Department Radio Call Signs	Number: ADM-24

Specialty Vehicles

Specialty vehicles shall be identified through Radio Call Signs as:

- Name of the unit followed by the assigned number of the vehicle (e.g., Marine 1, Air 3, and/or Cycle 5).
-

Portable Radio Call Signs

Members with a Fleet Designated Cruiser Number shall use that number when transmitting on the portable radio.

Members without a Fleet Designated Cruiser Number shall announce their name, rank, and ID number, if needed, while transmitting on the portable radio (e.g., members who are assigned to Troop "F").

Incident Command

The National Incident Management System (NIMS) has integrated existing best practices into a consistent, nationwide approach to domestic incident management at all jurisdictional levels and across functional disciplines.

Department member(s) involved at a critical incident with multiple agencies shall use a clear spoken message, based on common terminology.

References: MPAC: 81.2.4.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

1721

Department of State Police
General Order

Effective Date:	Number:
February 21, 2023	**ADM-25**
Subject:	
Paid Details and Overtime	

Policy

The Department may allow personnel, on full duty status or alternative duty status (as specified in ADM-11C Maternity Leave and Guidelines), to work paid details.

The Department recognizes the importance of maintaining safe and efficient traffic flow at roadway work sites and special events. The Department also recognizes that at major sporting, civic, special events, and other times, members may be required to provide crowd control and/or security.

Paid details may be worked by members:

- From the rank of Trooper through Detective Lieutenant inclusive; and/or
- From the rank of Captain/Detective Captain with approval of the Deputy Superintendent when:
  - The type of detail is "non-construction" i.e., stadium events, security details, in a supervisory capacity where they must supervise at least ten (10) officers; or
  - A vacancy exists on any type of detail after the primary and secondary detail lists of the respective troop have been completely exhausted of eligible members.
    Note: Once assigned to a detail, Captains/Detective Captains shall not be bumped by:
    1. Another Commissioned Officer; or
    2. A Non-Commissioned Officer or Trooper within twenty-four (24) hours of the start time of the assigned detail.

Definitions

Paid Detail Administrator: The Paid Detail Officer of jurisdiction or the point of contact for the Paid Details Management Service (PDMS) vendor. The Paid Detail Officer of jurisdiction, or the PDMS vendor, shall receive and coordinate paid detail requests, assignments, billing, collection, and compensation of payroll expenses.

Paid Detail: A voluntary assignment paid for by an outside entity, which has been authorized by the Colonel/Superintendent.

Scheduled Work Hours: A regular shift or tour of duty consisting of eight and one-half (8.5) hours.

Definitions, continued

Type I Paid Detail: A voluntary assignment requiring a commitment of up to four (4.0) hours duration paid for at a flat rate of four (4.0) hours of the detail rate, by an outside entity, which has been authorized by the Colonel/Superintendent.

Type II Paid Detail: A voluntary assignment requiring a commitment of up to eight (8.0) hours duration paid for at a flat rate of eight (8.0) hours of the detail rate, by an outside entity, which has been authorized by the Colonel/Superintendent.

Work: Shall be defined to include hours actually worked during regularly scheduled duty, overtime, court time and paid details.

Hours of Work

Members shall not schedule or work combinations of assignments and/or details which they know or should know will result in a direct violation of the "sixteen and one-half (16.5) hour rule" as contained within the Collective Bargaining Agreement (CBA) and this General Order (as further clarified in Superintendent's Memo *13-SM-10 Extension to the 16.5 Hour Rule Limitation*.)

Members shall not accept a detail or overtime assignment if doing so would require the member not to work a regularly scheduled shift or attend other work obligations of which the member is aware.

Members shall not cancel a detail in order to accept another detail or overtime assignment.

In the event the detail or overtime hours exceed the hours of work allowed in any twenty-four (24) hour period, the member shall not be allowed to alter the starting time of their next assigned work shift, but shall use accrued personal leave or vacation leave credits to offset any conflicts with their scheduled work hours.

Members shall be paid for details in conformance with their applicable collective bargaining agreement. When availability requirements or demand for a member working a Type I Paid Detail assignment goes beyond the four (4.0) hour duration, it shall automatically be converted to a Type II Paid Detail assignment. Any Type II Paid Detail assignment that goes beyond the eight (8.0) hour duration shall be extended in thirty (30) minute increments to be paid based on the hourly rate of time and one-half.

A member shall receive time and one-half detail pay for the actual hours worked on the calendar day of Thursday, Thanksgiving Day or December 25, Christmas Day.

Overlapping Time

There shall be no overlapping of details or overtime during the commitment times of the Type I or Type II Paid Details. This does not, however, preclude a member from beginning a regularly scheduled shift after being appropriately relieved from said detail and logging same in the Daily Administrative Journal.

In order to prevent any overlapping of scheduled work hours members shall utilize accrued personal or vacation leave to offset any overlap in conformance with the member's collective bargaining agreement.

Timely Recording of Paid Details

To ensure the timeliness of paid detail processing and to facilitate the use of PayStation for paid detail reporting members shall:

- Enter any detail hours worked into PayStation within twenty-four (24) hours of completion of the detail and prior to submitting PayStation for that week; and
- Paid details shall not be entered into PayStation prior to completion of the assignment.

Travel Time

Travel to/from a regularly scheduled shift to/from an overtime or detail assignment is expressly authorized, provided such travel does not exceed one-half hour from the geographical boundary of such regularly scheduled shift location. Personnel are on-duty during such periods of travel and shall undertake all necessary activities ordinarily performed during motor patrol. Members are required to use at a minimum, one-half (1/2) hour of accrued personal or vacation leave as travel time to or from a detail when the following occurs:

- The travel time from the duty assignment to the paid detail location or overtime assignment, or the paid detail to a duty assignment location, is **greater** than one-half (1/2) hour.
  Note: Members not assigned to a specific sub-station, the geographical boundary for a section/unit is defined as the station of jurisdiction where their **regular reporting** location is sited. Temporary Duty Assignments (TDY) work locations shall be considered as the member's regular reporting location for administration of this General Order.

When a member is assigned to a paid detail or overtime assignment they shall:

- Determine the need to use accrued personal or vacation leave to ensure prompt arrival to a detail or when reporting for their tour of duty or overtime assignment; or
- Decline the detail/overtime assignment if they chose **not to use** the appropriate accrued personal or vacation leave.

Supervisors shall be held responsible:

- To ensure members are held accountable for taking appropriate accrued personal or vacation leave when reporting to or from a paid detail/overtime, if it effects their regular tour of duty assignment; and
- To ensure members accurately document and record accrued person or vacation leave used for travel time to or from a paid detail/overtime when **greater** than one-half (1/2) hour

Requests

Members shall not:

- Make duplicate/same day requests for details in different Troops; or
- Request or work overtime or details within twenty-four (24) hours from the start time of their regularly scheduled work shift when sick leave was taken for:
  - Personal illness or injury;
  - The presence of the member at their work location would jeopardize the health of others, through exposure to a contagious condition; or
  - The member's spouse, child, parent, or spouse's parent, or relative living in the member's household, is seriously ill. In this event, a limit to the amount of leave the member can use is set by the CBA and federal and state laws.

Exception: A member who works at least four (4) or more consecutive hours of their regularly scheduled work shift, in which Sick Leave was granted as outlined in ADM-11 Sick Leave, shall remain eligible to work paid details and overtime.

Members may request only one troop as a primary choice on an SPD-3 Request for Paid Detail form. The primary choice for:

- Members assigned to Field Operations within the Division of Field Services shall be limited to the troop to which they are assigned, or to the troop where they reside;
- Members assigned to the Division of Field Services, but not assigned to a troop within Field Operations, may request any troop as their primary choice; and
- Troop F is reserved for members assigned to: Troop F, Office of the Superintendent, Division of Field Services (see above), Division of Administrative Services, Division of Investigative Services, Division of Standards and Training, the Division of Homeland Security and Preparedness, and Forensic Services Division.

If a member wishes to change their primary choice, the SPD-3 shall be forwarded to the Paid Detail Administrator of jurisdiction prior to the first of March each year or upon transfer.

Weekly requests for assignments shall be made according to a procedure approved by the Troop Commander. When requesting a detail, a member shall report all out-of-troop details worked for the previous five (5) weeks to the Paid Detail Administrator of jurisdiction.

Member Responsibilities

Members assigned to a road construction type detail shall maintain a professional presence and shall perform the following duties:

- Provide public and site safety;
- Be aware of, and visible to, oncoming traffic;

- Maintain uniform traffic flow through manual direction or other devices as necessary;

Member Responsibilities, continued

- Stand, facing traffic, unless otherwise directed or authorized;
- Wear proper field uniform and assigned traffic vest or raincoat with high visibility side out;
- Remain on the work site, except to perform enforcement duties, or at the direction of the state engineer, site foreman, appropriate authority, or in case of personal necessity; and
- Maintain radio contact with Troop of jurisdiction.

If radio contact is not possible with the Troop of jurisdiction, then contact the nearest troop or station.

If more than one member is assigned to a detail, then the members shall:

- Position themselves uniformly throughout the site or as directed by the state engineer, site foreman, or appropriate authority; and
- Dress alike, in the duty uniform of the day, or as prescribed by the officer-in-charge (OIC).

Members shall:

- Arrive and depart at the times posted and/or prescribed by the Paid Detail Administrator, state engineer, site foreman, or appropriate authority;
- Appropriately record the start time and end time of the paid detail, the actual hours worked, the hours to be paid, the location, and the contractor name;
- Enter into PayStation the detail information including the total amount of hours to be paid; and
- Enter into the PayStation "Comments" field the detail start and end time and the actual hours worked.

Members assigned to a detail shall appropriately report the start time and end time of the paid detail, the actual hours worked, the hours to be paid, the location, and the contractor name to both:

- The Paid Detail Administrator of jurisdiction; and
- The supervisor authorizing the member's PayStation entries: and

When a member is assigned a detail <u>outside</u> of that member's primary troop choice, the member shall furnish the above information to the member's primary Troop Paid Detail Administrator.

Failure to adhere to the requirements outlined in this General Order shall constitute unsatisfactory performance and the member may be disciplined under the Department Rules and Regulations. In such instances the member may be removed from all detail lists until final disposition of the formal disciplinary process.

Supervisory Responsibilities

All supervisory personnel shall:

- Monitor all members assigned to details;
- Immediately address and remedy all observed violations of this General Order; and
- Document all violations on the SP 381 Paid Detail Inspection form, prior to the end of that shift.

The supervisor approving a member's weekly PayStation entry shall:

- Review the member's submitted record of paid details/overtime worked;
- Review the weekly entries made by the member in PayStation;
- Ensure that the submitted record of paid details/overtime worked corresponds correctly to the PayStation weekly entries;
- Require the member to use accrued personal or vacation leave in order to ensure compliance with this General Order; and
- Report all violations of hours to their Commanding Officer.

Troop Commanders

Troop Commanders are directly responsible for the administration and supervision of this General Order and shall assign a supervisor to:

- Conduct inspections of detail sites within the Troop jurisdiction; and
- Submit SP-381 forms with all applicable findings.

Troop Commanders/Duty Officers of jurisdiction over the detail shall only authorize members to work in excess of 16.5 hours when:

- An emergency situation has arisen that requires the members' presence; or
- The member is on their last scheduled work day; or
- The member is on a day off and has no scheduling conflict.

Extension to the 16.5 Hour Rule

The Troop Commander or Troop Duty Officer of jurisdiction over the detail may grant an extension in order to allow member(s) to extend beyond the sixteen and one-half (16.5) hour limit under the following conditions:

- Member(s) shall not be granted more than one extension to the 16.5 hour rule in any forty-eight (48) hour period; and
- No more than a two (2) hour extension shall be granted without the member being required to take paid leave time, (vacation, personal), to ensure adequate rest before the start of their next assignment.

In no event shall the maximum number of weekly work hours as allowed by the Collective Bargaining Agreement be exceeded. Please refer to Superintendent's Memo *13-SM-10 Extension to the 16.5 Hour Rule Limitation* for further clarification.

Troop Inspections

The Troop Executive Officer shall maintain all SP-381 forms and ensure that those forms indicating unsatisfactory performance are brought to the attention of the Troop Commander.

Troop Inspections shall include:

- Site, time, members present, overall appearance, adherence to General Order;
- Verification of assigned members arrival and departure times with both the record of paid details worked and state engineer and/or site foreman; and
- Detail violation(s), if any.

Staff Inspections

Staff Inspectors shall conduct random inspections of detail sites and submit written reports to the appropriate Troop Commander of findings and recommendations to include:

- Site, time, members present, overall appearance, adherence to General Order;
- Verification of assigned members arrival and departure times with both the record of paid details worked and state engineer and/or site foreman;
- Detail violation(s), if any;
- Audit of actual and overall hours worked by assigned members;
- Audit of Paid Detail Office, and
- Audit of Paid Detail Administrator's reports

Administration

Troop Commanders shall issue a Troop Commander's Order outlining the administration of paid details in their respective troop. Troop Commanders shall assign a supervisor as the Paid Detail Officer.

The Paid Detail Officer shall:

- Work an administrative day shift or eve shift at the direction of the Troop Commander;
    - Ensure the administration of paid details complies with the Troop Commander's Order.

Cruisers

The Paid Detail Officer with the approval of the Troop Commander shall determine the number of vehicles at details.

Marked and unmarked vehicles shall:

- Have working emergency lighting activated, when appropriate;
- Be conspicuously and strategically placed between oncoming traffic and the work site; and
- Be properly fueled prior to the detail.

Undercover vehicles shall not be used at road construction sites.

Commercial Motor Vehicle Escort Details

Prior to an escort detail, a member assigned to the Commercial Vehicle Enforcement Section, or the member assigned to the detail, shall inspect all oversized or overweight loads for:

- Permits;
- Load security;
- Vehicle condition; and
- Operator qualifications.

Breaks

To minimize impact on the work site, breaks shall be taken:

- At scheduled times in conjunction with vendor's/contractor's scheduled breaks; and
- Out of public view whenever possible.

References:

ADM-11 Sick Leave;
ADM-11C Maternity Leave and Guidelines;
10-SM-04 Rank of Captain and Detective Captain Working Paid Details;
07-SM-09 Utilization of Leave Time;
20-SM-16 Timely Recording of Paid Details;
SPAM Unit 5A-Commonwealth CBA, Comm-SPAM Executed on the Record 2018-2020 12-2-19;
SPAM Unit 5A-Commonwealth CBA, Comm-SPAM Executed 2018-2020 MOA 7-31-20;
13-SM-10 Extension to the 16.5 Hour Rule Limitation;
SPD-3 Request for Paid Detail Form;
SP 189 Court Card;
SP 381 Paid Detail Inspection Form.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

1720

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**ADM-26**
Subject:	
Military Service	

Policy

The Department shall allow sworn and civilian employees who are members of a Reserve Component of the United States Armed Forces (i.e., the Army National Guard of the United States, the Air National Guard of the United States, the Army Reserve, the Navy Reserve, the Marine Corps Reserve, the Air Force Reserve, and the Coast Guard Reserve) to attend drills and other training as required.

The Department shall allow employees who are members of the Massachusetts Army and Air National Guard and called to emergency/contingency duty in the service of the Commonwealth, to perform their required duties in accordance with the provisions of M.G.L. c. 33, Sections 38, 40, 41, 59, 59A, 60 and 61, and perform duties under Title 10 and 32 of the United States Code (USC).

The Department shall allow employees who are members of the Army and Air National Guard of other states or U.S. territories, to perform active duty as required by the proper authority of the other state or territory.

The Department shall support and facilitate the transition of employees who are called to active service under USC Title 10 and Title 32 upon their activation/mobilization as well as their return from active duty. This supported transition will ensure that the employee is treated fairly and equitably in accordance with all applicable federal and Massachusetts state laws pertaining to their service and employment rights.

Purpose

To establish and define military service protocols for Department of State Police personnel.

Notifications

Employees shall notify Station, Section and/or Unit Commanders of Inactive Duty Training Drill (IDT Drill), Annual Training, emergency/contingency activation/mobilization, as well as any other service obligations that conflict with regular work schedules with as much advance notice as possible.

Notifications Procedure

Members receiving military orders, yearly drill schedules and military leave earning statements shall adhere to the following notification procedure:

- All military orders, yearly drill schedules, and military leave earning statements (LES) shall be submitted via email to polmilitaryleave@pol.state.ma.us. immediately upon notification of military activation if eligible for pay difference during any portion of that military service.
- All military service orders and drill schedules will be reviewed by the Department's Human Resources Military Service Coordinator. Based on the military orders submitted, instructions will be provided to the employee and supervisor to ensure the proper weekly time reporting codes are utilized during the employee's military service. Payroll will not process any paid military service selections in the time reporting system without having received current military orders or drill schedules.
- Until documentation is received and reviewed by the Human Resources Military Service Coordinator, the employee's payroll status will be "Military Leave/No Pay." Additionally, timely notice of pending military service shall be made through the chain of command via a "To/From." The notice shall include:
  - The timing and purpose of military service;
  - Reference of any applicable law; and
  - A copy of official orders or correspondence on official letterhead.
- In the event the employee has not received written orders in hand, the employee shall submit notification through the chain of command to the Office of the Superintendent/Deputy Superintendent and polmilitaryleave@pol.state.ma.us with the following additional information:
  - The name and rank of the military commanding officer;
  - A contact phone number for the commanding officer; and
  - Notice that written orders will be forthcoming.

Time Reporting

Employees on Military Leave With or Without Pay shall be placed on an administrative schedule (i.e., a 5 and 2 schedule) for the duration of any individual or consecutive leaves in excess of thirty (30) consecutive/calendar days. All pertinent station, section, and/or unit records must reflect such schedule. Please note that employees who are performing annual training, drill, or related assemblies do not require this schedule change.

Station, Section, and/or Unit Commanders shall ensure that the appropriate notations are entered into the time reporting system to reflect the employee's military leave/work status if the employee is unavailable to do so.

Authorized Leave

Refer to the accompanying ADM-26 Military Leave – Matrix that is incorporated into this policy.

Department Work While on Military Leave

While an employee is on a military leave of any duration, the employee shall:

- Be deemed separated from service with the Department; and
- Not work any overtime assignments, detail assignments, or be compelled by the Department to perform any other function on behalf of the Department or in the capacity of a Department employee.

Leave Accrual, Seniority, and Other Pay Considerations for Employees on Military Leave

Employees who are called to military service that qualifies them for Military Leave With Pay (pursuant to M.G.L. c. 33, §38, 40 or 41) or Without Pay (under Title 10 or 32 USC or for service with the National Guard of another state or U.S. territory pursuant to M.G.L. c. 33, §13), shall:

- Retain all employment rights pursuant to federal and Massachusetts state law;
- Suffer no loss of Department seniority or seniority for retirement purposes;
- Continue to accrue all regularly accrued paid leave time (sick, vacation, and personal leave) as though still present for duty;
- Leave accrued while on active military leave status cannot be applied to that same unpaid military leave;
- Leave accrued while on active military leave status cannot, upon the employee's return to work, be applied retroactively to result in compensation for previously unpaid leave time;
- Employees on military leave without pay may request to use compensatory time and paid leave time accrued prior to the onset of the military leave without pay as a substitute for unpaid leave, provided that the employee does not qualify to receive a pay difference. Such use of compensatory time earned and accrued leave shall be in accordance with regularly applied rules for use as set forth in the applicable CBA and Policies & Procedures;
- Personal leave accrued while on military leave remains use or lose time for that calendar year. There is no carry-over of personal leave;
- Vacation leave accrued while on military leave remains subject to annual carryover rules per the applicable CBA and state policies; and
- Employees on military leave with pay are only entitled to pay for benefits that are seniority based, not performance based, unless otherwise specified in the applicable CBA. (e.g., shift differential, weekend differential, commuting differential, on-call or stand-by pay, clothing allowance, etc.).

Holidays and Administrative Days Off for Employees on Military Leave

Employees in the armed forces of the Commonwealth on Military Leave With Pay due to activation under M.G.L. c. 33, §§ 38, 40 and/or 41 shall receive holiday pay as regularly compensated per the applicable CBA and state policies, however they shall not be eligible to accrue compensatory time or "holidays owed." On the Commonwealth's day of observance, the payroll code for "Holiday – Did Not Work" shall be entered into the time reporting system and recorded accordingly in station, section, and unit records for the employee.

In accordance with the applicable CBA and state policies, employees who are on Military Leave Without Pay shall not receive holiday pay and are therefore not eligible for accrual of compensatory time or "holidays owed" for legal holidays that occur while the employee is in leave of absence without pay status. Please be advised that the military pay difference for an employee in Military Leave Without Pay status does include compensation for holidays that occur during the leave period.

Administrative Days Off (ADOs) are equivalent to Days Off Regular and shall not be accrued.

Time Limit for Return to Work

Time limits for returning to work from military service depend on the duration of the orders. The rules are:

Service of 1 – 30 days: the beginning of the next regularly scheduled work period on the first full day following completion of service and expiration of an eight-hour rest period.

Service of 31 – 180 days: application for reinstatement to duty through chain of command in To/From format to the Office of the Superintendent/Deputy Superintendent shall be submitted not later than 14 days after completion of military duty.

Service of 181 or more days: application for reinstatement to duty through chain of command in To/From format to the Office of the Superintendent/Deputy Superintendent shall be submitted not later than 90 days after completion of military duty.

In the event an employee does not return to work in a timely manner, he/she is subject to the Department's Rules and Regulations, Policies and Procedures, and applicable provisions of the relevant CBA for unauthorized absences.

Sworn Member Requirements for Return to Department Service

Any leave or break in service 90 days – 1 year:

Members returning from any leave, temporary modified duty or break in service exceeding ninety (90) days requesting full duty status shall ensure the tasks below are completed in the following sequence:

- The members' Station / Section / Unit Commander shall notify Human Resources in advance of date of return and request the member is returned to full duty;
- Human Resources will notify the Division of Standards and Training Commander or designee when the member is returned to full duty;
- The member shall then be required to successfully complete:
  - Online academy;
  - Refresher training in the following areas (if deemed necessary by the Division of Standards and Training Commander or designee):
    1. Patrol Procedures
    2. Defensive Tactics
    3. EVOC
    4. Firearms (reissuance of assigned UOF gear and requalification if necessary)
- Upon satisfactory completion of training, the Station / Section / Unit Commanders will be advised by the Commandant of the State Police Academy.

Any leave or break in service exceeding 1 year:

Members returning from any leave or break in service exceeding one (1) year requesting full duty status shall ensure the tasks below are completed in the following sequence:

The members' Station / Section / Unit Commander shall notify Human Resources in advance of date of return and request the member is returned to full duty.

- The member shall then be required to successfully complete:
  - A background investigation;
  - A medical examination by the State Police Surgeon to include drug testing; and
  - Psychological testing.

Human Resources will notify the Division of Standards and Training Commander or designee when the member is returned to full duty.

The member shall then be required to successfully complete:

- Online academy
- Refresher training in the following areas (if deemed necessary by the Division of Standards and Training Commander or designee):
  - Patrol Procedures
  - Defensive Tactics
  - EVOC

Sworn Member Requirements for Return to Department Service, continued

- Firearms (reissuance of assigned UOF gear and requalification if necessary)

- Upon satisfactory completion of training, the Station / Section / Unit Commanders will be advised by the Commandant of the State Police Academy.

Former members wishing to return from a separation from service that exceeds three (3) years shall:

- Meet all requirements for re-entry to the Department; and
- Successfully complete the Recruit Training for appointment to the position of Trooper.

Note: Failure to successfully complete the Recruit Training may affect pension benefits, if applicable.

Civilian Employee Requirements for Return to Department Service

Civilian employees returning from any military leave that exceeds one year shall be required to successfully complete:

- A background investigation;
- A medical examination, to include drug testing, by the State Police Surgeon;
- Psychological testing; and
- Retraining, as determined by the employee's supervisor or the Human Resources Director.

References:

Commonwealth Collective Bargaining Agreements:

- AFSCME Unit 2-Commonwealth CBA, Article 8, § 7;
- MCOFU Unit 4-Commonwealth CBA, Article 8, § 6;
- MOSES Unit 9-Commonwealth CBA, Article 8, § 6;
- NAGE Units 1, 3 and 6-Commonwealth CBA, Article 8, § 6;
- SPAM Unit 5A-Commonwealth CBA, Article 8, §2.c., Article 38, §§ 3.

MGL c. 33, §§ 38, 40, 41, 59, 59A, 60, and 61;
National Defense Act of 1933;
Rules Governing Paid Leave for Managers and Confidential Employees (HRD Red Book);
Title 10 USC, c. 11, § 270 Title 32 USC (National Guard);
Title 38 USC, c. 43, §§ 4301-4333 (USERRA);
MPAC: 22.2.1.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
December 6, 2022	**ADM-27**
Subject:	
Transfers	

Policy

In order to maintain and enhance the operational functions of the Department, transfers may be made to:

- Ensure adequate staffing levels;
- Provide efficient public safety services; and
- Meet other goals and objectives of the Department.

Transfer Restrictions

Troopers assigned to the Division of Field Services, who have three (3) or fewer years of creditable service shall not be considered for any job posting or positions outside of the Division of Field Services.

This restriction does not preclude the Colonel/Superintendent from assigning Troopers with three (3) or fewer years of creditable service to positions outside of the Division of Field Services based upon specific expertise (e.g. language skills, etc.) which a Trooper may possess.

Troopers with five (5) or more years of creditable service may bid on positions within the Division of Field Services-Field Operations pursuant to the Collective Bargaining Agreement.

Biddable Assignments

Biddable Assignments: All assignments established as a biddable assignment pursuant to the Collective Bargaining Agreement.

Non-Biddable Assignments

Non-biddable Assignments: All assignments not otherwise established as a biddable assignment pursuant to the Collective Bargaining Agreement.

Department non-biddable assignments include, but are not limited to:

- Division of Investigative Services;
- Division of Administrative Services;
- Division of Standards and Training;
- Division of Homeland Security and Preparedness;
- Forensic Services Division
- Division of Field Services pursuant to the Collective Bargaining Agreement, and
- Office of the Superintendent.

Non-Biddable Assignments, continued

Due to the specialized nature of these assignments, and the knowledge and skills required, these positions require a selection process.

Request for Transfer: Biddable Assignments

Members who request a transfer to a biddable assignment within the Division of Field Services shall:

- Submit an electronic transfer request.

Only those requests received at least twenty-one (21) days prior to the end of a fifty-six (56) day bid cycle shall be considered for the next fifty-six (56) day bid cycle.

Members are allowed to have only one (1) transfer request for a biddable assignment at any time.

The Human Resources Section shall publish a list of transfer requests for the Division of Field Services on Docushare containing the requesting member's name, current assignment, request, and seniority. Two (2) lists shall be maintained: one (1) list for troopers and one (1) list for supervisors.

Note: Requests for transfers to a biddable assignment within the Division of Field Services shall remain on file until honored or withdrawn.

Request for Transfer: Non-Biddable Assignments

Members who request a transfer to a non-biddable assignment within the Department shall submit the following to Human Resources Section:

- A To/From;
- A resume; and
- Any other materials required within the posting.

The member shall forward a copy of the above items to:

- Their current Commanding Officer; and
- The Commanding Officer of the requested section/unit.

Requests for transfer to a non-biddable assignment shall not be kept on file at the Human Resources Section. All requests shall be submitted within the specified time periods of the posting.

Members who request a transfer to a non-biddable assignment within their respective troop or station shall submit the following to the Troop Commander:

- To-From;
- Resume; and
- Any other materials required within the posting.

Posting and Selection Process: Non-biddable Assignments

Vacancies for non-biddable assignments for members shall be posted for at least ten (10) calendar days on Docushare.

Providing that the minimum qualifications are met, members may apply to:

- Department non-biddable assignments;
- Troop non-biddable assignments when the member is assigned to the troop; and
- Station non-biddable assignments when the member is assigned to the station.

Each posting shall include:

- Assignment, location, and work schedule;
- Name of the current Commanding Officer;
- Rank requirements, if any;
- Minimum commitment and retention requirements, if any (e.g., completion of specialized training or the ability to develop a specialized skill); and
- Other requirements or information as appropriate.

Note: All qualified applicants shall be considered. Members who are on leave are responsible for keeping themselves informed of such postings.

Department Procedure: Non-biddable Posting and Selection

Step	Action
1	The Commanding Officer of the section/unit shall seek approval to fill the vacancy from their Division Commander.
2	The Division Commander shall seek approval to fill the vacancy from the Deputy Superintendent.
3	The Division Commander shall submit a SP 389 Posting Request form to the Human Resources Section for any anticipated openings.
4	The Human Resources Section shall post the anticipated openings for non-biddable assignments for ten (10) calendar days.
5	The Human Resources Section shall forward all timely non-biddable transfer requests to the Section/Unit Commander for review.

Department Procedure: Non-biddable Posting and Selection, continued

Step	Action
6	The Commanding Officer of the section/unit shall schedule interviews, conduct the selection process, and select the candidate(s).
7	The Commanding Officer of the section/unit shall submit a To/From to the Division Commander detailing: • The names of all applicants; • The names of the qualified applicants interviewed, the members of the interview panel, questions asked, and the evaluation instrument; and • The candidate chosen. The chosen candidate's resume and other applicable documentation shall be attached to the To/From.
8	If the Commanding Officer of the section/unit does not find an acceptable candidate, the position may be posted again using the process identified above.
9	The transfer order shall serve as official notice to the candidate(s).

Department Procedure: Troop and Station Non-biddable Posting and Selection

Step	Action
1	The Troop Commander shall post within the troop for ten (10) calendar days for anticipated openings for troop/station non-biddable assignments.
2	The Troop Commander, along with the Commanding Officer of the section/unit where applicable, shall review submissions, schedule interviews, conduct the selection process, and select the candidate(s).
3	If the Troop Commander does not find an acceptable candidate, the position may be posted again using the process identified above.
4	The transfer order shall serve as official notice to the candidate(s).

Interview Process: Non-biddable Assignments

Commanding Officers shall:

- Create an interview panel with a minimum of two (2) people;
- Create a list of standard questions using guidelines from the Human Resources Section; and
- Ensure that a minimum of three (3) qualified applicants are interviewed using the standard questions referenced above. (Follow-up questions may be asked, as necessary.)

If there are less than three (3) qualified applicants, all qualified applicants shall be interviewed.

If the section/unit works in conjunction with another agency (e.g., District Attorney's Office), a representative of the other agency may be one of the interview panel members.

Responsibilities

Position	Duties
Deputy Superintendent	• Schedule transfer meetings as needed; • Obtain the transfer request list from the Human Resources Section and conduct inter-divisional transfer meetings; • Review candidates and the operational needs of the Department; • Make written recommendations for transfers to the Colonel/Superintendent; and • Notify Commanding Officers of pending transfers.
Colonel / Superintendent	• Review and approve or deny the recommendations for transfer; and • Forward the approved transfers to the Human Resources Section.
Human Resources Section	• Issue transfer orders through the Office of the Colonel/Superintendent; and • At least five (5) days before the transfers become effective, notify all members affected by the transfers, through transfer orders.

Transfer Process	Transfer meetings shall take place in conjunction with the fifty-six (56) day bid cycle. Commanding Officers shall be immediately notified of the finalized transfers. Transfers shall be effective seven (7) days prior to the end of the current 56-day bid cycle. Commanding Officers may make transfers outside of the fifty-six (56) bid cycle based on operational needs of the Department.
Bidding and Bid Cycle	All bidding shall conform to the Collective Bargaining Agreement. Once in effect, the fifty-six (56) day bid cycle shall not be violated. Exceptions are as follows: • Promotions; • Training activities, with five (5) day-notice given to the affected member; • Vacancies created as a result of retirement, illness, or leave; • Emergencies; or • With the mutual consent of all parties.
Intra-Troop/Division Transfers	Troop and Division Commanders may make transfers within their Troop or Division at any time within the guidelines of this policy. Troop and Division Commanders shall notify their respective commanders and the Human Resources Section of the pending transfers.
Temporary Duty (TDY) Assignments	TDY assignments may be made by the Colonel/Superintendent at any time. TDY assignments: • Need not be posted; and • Shall not exceed ninety (90) days without a review and written extension by the Colonel/Superintendent. Members shall maintain only one (1) TDY status at any given time. Troop Commanders may make TDY assignments within their troop and shall forward a copy of the order to the Human Resources Section.

Deployment	Each Division Commander shall conduct a needs assessment in order to deploy personnel in the best interests of the Department. The Human Resources Section shall maintain a Position Management System that contains: • A table of organizational entities, as approved by the Colonel/Superintendent; • A position description, classification, and task analysis; • The number, type, and location of each position; and • A monthly report indicating whether each position is filled or vacant.
Supervisory Members	Supervisory members do not have bidding rights but may be considered for posted positions in accordance with the process identified in this policy.
Equal Opportunity	The Diversity Officer shall obtain and review transfer request lists from the Human Resources Section. The Diversity Officer may make recommendations in writing to the Colonel/Superintendent.

References: MGL Ch. 22C;
SPAM Collective Bargaining Agreement Article 28;
SP 389 Posting Request Form;
SP 389A Troop Posting Request Form.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

1742

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**ADM-28**

Subject:

Department Motor Vehicles

Policy

State owned vehicles shall be operated for official use only and in accordance with Policy and Procedure ADM-19 *Vehicle Management,* ADM-19A *Vehicle Use and Maintenance and ADM-19B Automated Vehicle Locator (AVL) Technology*.

Commuting in Cruisers

Members with cruisers who are traveling to and from home to their duty stations or assignments shall undertake all necessary activities ordinarily performed during motor patrol.

While commuting in a cruiser, all members are to be attired in the required duty uniform unless their usual duties require otherwise.

While commuting with a cruiser, discretion in choosing routes of travel should be used in order to promote the visibility concept on roadways which receive little or no coverage.

A member coming upon an accident scene while in commuting capacity shall immediately notify the substation or police agency of jurisdiction. The member shall then assist at the scene until relieved by an officer from the substation or police agency with primary jurisdiction, or receives instructions to take appropriate action. If the accident occurs on a roadway where the State Police has primary jurisdiction and a State Police patrol is not available, he/she shall investigate the accident, advise the substation having jurisdiction of the pertinent details, and make a report of same upon returning to duty.

A commuting member arriving at his/her residence shall ensure that the cruiser is properly secured in a safe place and that all equipment is secured in a locked compartment within the cruiser. Firearms shall not be left in an unattended cruiser unless secured in accordance with UOF-04 *Use of Force Equipment*. The vehicle, whenever possible, shall not be parked on a public way. A member may garage a cruiser, at no expense to the Commonwealth, away from his/her residence if the Troop or Section Commander approves the location.

Members shall be required to commute in cruisers, when available, to and from their duty stations and/or assignments and homes, between shifts, unless otherwise authorized by the Troop or Section Commanding Officer.

Subject: Department Motor Vehicles	Number: ADM-28

Vehicle Maintenance

Members shall ensure that cruisers assigned to them are given proper maintenance and care. Members shall also ensure that expended or faulty emergency and safety equipment is promptly replaced. Before returning from days off and starting a tour of duty each member shall inspect the cruiser assigned to them in order to determine if the vehicle is in good condition, undamaged and that all equipment prescribed for the vehicle is present and operable. Any deficiencies shall be recorded in the Barracks Daily Administrative Journal/Department Records Management System and corrective action shall be initiated by the member.

Vandalism to an unattended cruiser shall be reported to the member's duty station or assignment as soon as possible after discovery. Any damage to a cruiser or its equipment, sustained while commuting, responding, or on recall, shall be reported as prescribed for regular on-duty status.

References

ADM-19 Vehicle Management;
ADM-19A Vehicle Use and Maintenance;
ADM-19B Automated Vehicle Locator (AVL) Technology;
UOF-04 Use of Force Equipment.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**ADM-29**
Subject:	
Workplace Violence	

Policy

The Department shall maintain zero tolerance for workplace violence and shall ensure that the workplace environment remains free from any form of violence.

This policy shall be applicable to all employees, sworn and civilian.

This policy does not apply to situations where sworn members are exposed to threats or violent acts from persons in their care or custody, or the public at large, as an unavoidable component of the lawful performance of their law enforcement duties.

Workplace Violence Defined

Workplace shall be defined as:

- Any Commonwealth owned or leased property;
- Any location where Commonwealth business is conducted;
- Any site where an employee is considered on duty;
- Commonwealth vehicles or private vehicles being used for Commonwealth business; or
- Any location if the violence has resulted from an act or decision made during the course of conducting Commonwealth business.

Workplace violence shall include, but is not limited to:

- Intimidation or threats communicated by any means;
- Physical assault and/or battery;
- Threats and/or acts of intimidation communicated by any means that cause an employee to be in fear of their own safety;
- Disruptive or aggressive behavior that causes a reasonable person to be in fear of their own safety or that of a colleague or that causes the disruption of workplace productivity; or
- Property damage.

Incidents of workplace violence may be individual acts or may take place between an employee(s) and:

- Other employee(s);
- Clients/customers/vendors;
- Acquaintances/partners; and
- The general public.

Workplace Violence Coordinator

The Workplace Violence Coordinator shall be a Commissioned Officer assigned by the Colonel/Superintendent. The Workplace Violence Coordinator shall report directly to the Commanding Officer of the Division of Standards and Training.

Workplace Violence Safety Incident Team

The Deputy Superintendent shall designate employees to the Workplace Violence Safety Incidence Team and provide such names to the Commonwealth's Human Resource Division. The established team shall consist of:

- A Commissioned Officer or senior manager from each division; and
- Representation from the Department's Human Resources Section, the Office of Employee Relations, Division of Standards and Training, and the Legal Section.

Disciplinary Action

Any employee found to have engaged in any act of workplace violence, in violation of this policy, is subject to disciplinary action up to and including termination.

Disciplinary action may also require the employee to participate and to successfully complete counseling, anger management education, or other appropriate programs.

The Department may consider acts of workplace violence, along with an employee's success in completing recommended programs, within the promotional process and other work related determinations (where not prohibited by statute, regulation or collective bargaining agreement).

Investigations

The Workplace Violence Coordinator does not conduct investigations into workplace violence. All investigations shall be conducted in accordance with ADM-14 Personnel Investigations.

Responsibilities

Position	Duties
Department Employees shall:	• Not engage in workplace violence behavior; • Immediately report any incident, threat of incident, or potential incident of workplace violence to their immediate supervisor; • Cooperate in investigations of workplace violence; and • Actively participate in the Department's efforts to prevent and eliminate workplace violence.
Sworn Members shall:	• Promptly respond to reports of workplace violence; • Take appropriate and immediate enforcement action in response to an incident to ensure the safety of those involved; • Follow proper reporting and investigating procedures as prescribed by this policy; and • Make notification to the Workplace Violence Coordinator, **within seventy-two (72) hours of the incident** utilizing a SP 390 Workplace Violence Incident Report.
Supervisors shall:	• Aggressively monitor the workplace to prevent and detect workplace violence; • Take appropriate corrective action to stop workplace violence; • Immediately report any incident of workplace violence to the Troop/Section Duty Officer and the Workplace Violence Safety Incidence Team Member designated for their Division; • Conduct investigations in a manner that is sensitive to the safety concerns and privacy of the victim(s), the perpetrator(s), and all witnesses; • Assist the employee/victim of a workplace violence incident by providing any additional support or services necessary to ensure their protection and safety; • Forward a copy of the final report for all workplace violence incidents, through channels, to the Workplace Violence Coordinator; • Make appropriate referrals to the Employee Assistance Unit, the Office of the Ombudsman, or Human Resources Section as needed; and • Ensure notification is made to the Workplace Violence Coordinator, **within seventy-two (72) hours of the incident** utilizing a SP 390.

Responsibilities, continued

Position	Duties
Station/ Section/ Unit Commanders shall:	• Ensure, if necessary, written workplace protection plans are devised for employee(s) who are victims of workplace violence; and • File a copy of the workplace protection plan with the Workplace Violence Coordinator.
Workplace Violence Safety Incident Team shall:	• Meet as needed, to devise, review policies, procedures and safety protocols for workplace violence; • Ensure, when necessary, written workplace protection plans for employees who are victims of workplace violence are operative; • Ensure consistent and coordinated responses to acts of workplace violence; • Evaluate and/or make additional notification, recommendations as required when notified of an incident of workplace violence by a supervisor; and • Review and evaluate any serious or critical incidents of workplace violence and make any appropriate recommendations to the Workplace Violence Coordinator necessary to enhance safety considerations.
Workplace Violence Coordinator shall:	• Review and file all final reports of workplace violence incidents and make recommendations to the Division Commander of Standards and Training and the Workplace Violence Safety Incident Team; • Coordinate and schedule meetings as needed with the Workplace Violence Safety Incident Team; and • Annually report statistical data relative to workplace violence incidents within the Department to the Division Commander of Standards and Training.
Human Resources Section shall:	• Coordinate with Workplace Violence Coordinator and the Commonwealth's Human Resources Division regarding Workplace Violence Training; and • Maintain all records of civilian employees trained in workplace violence.

Subject: Workplace Violence	Number: ADM-29

Exceptions	All employees should be aware that conversations with the Office of the Ombudsman and/or Employee Assistance Unit are considered confidential and that these entities are not the proper venue for notification to the Department for workplace violence complaints or incidents.
Retaliation	Any retaliation against an individual who has complained about workplace violence and any retaliation against individuals for cooperating with an investigation of workplace violence are prohibited and shall not be tolerated.
Distribution of Policy	This policy shall be issued to each employee upon hiring, and shall be continuously posted and available on PowerDMS.

References: ADM-14 Personnel Investigations;
SUP-04 Employee Assistance Unit;
SUP-12 Office of the Ombudsman;
Executive Order No. 442; SP 390 Workplace Violence Incident Report;
SPAM Collective Bargaining Agreement Article 27.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**ADM-30**
Subject:	
Asset Management	

Policy

The Department shall conduct an Annual Fixed Asset Inventory.

The Department shall:

- Record and report Governmental Generally Accepted Accounting Principles (GAAP) Fixed Assets of $50,000 or more within the Massachusetts Management Accounting and Reporting System (MMARS) twice per year pursuant to State Comptroller policy;
- Maintain an Asset Management System that reflects all Non-GAAP Fixed Assets with a useful life of one (1) year or more and a cost between $1,000 -$49,999; and
- Maintain inventories of other assets in accordance with State Comptroller policy and as determined by the Division of Administrative Services.

Definitions

Asset Forfeiture or Federal Grant Fixed Asset: Tangible property funded with asset forfeiture or federal grant funds with a useful life of (1) one year or more, regardless of original cost.

Fixed Assets: Tangible property with a cost of $1,000 or more and a useful life of one (1) year or more.

Technology Asset: Tangible asset determined to have the capability of storing data, regardless of original cost (excludes USB flash drives, digital versatile disks, or other consumable technology).

Asset Management

The Asset Management Unit shall manage fixed asset transactions and conduct an annual inventory.

The Division of Administrative Services Chief Administrative Officer or designee shall:

- Designate the Asset Manager for the Department; and
- Ensure the Asset Management Unit reports to the Division of Administrative Services Chief Administrative Officer or designee.

Asset Management, continued

When Commanding Officers acquire, transfer, lose, or dispose of fixed assets, they shall:

- Notify the Asset Management Unit by forwarding a copy of the SP 255 Equipment Transfer Form or by providing information via email.

Annual Fixed Assets, Biannual Capital Assets Inventories, Asset Forfeiture, Technology, and Federal Grant Inventories

Step	Action
1	The Asset Management Unit shall provide a report of the inventory to the Commanding Officer of each reporting entity.
2	Commanding Officers shall: • Reconcile the inventory with their previous inventory by physically accounting for each item listed; • Complete and return the SP 255 form for fixed assets that have been acquired, transferred, lost, or disposed of; • Complete and return the SP 255A form for all disposals; this form is in addition to the SP 255 form; • Tag newly acquired items with an inventory control identification number; • Rectify discrepancies; • Retain copies of the inventory printout and SP 255 and SP 255A forms; • Sign-off on Capital (Fixed) Asset Inventory confirmation sheet for biannual review of GAAP Fixed Assets; • Complete, sign, and return Compliance letter for annual inventory reviews; and • Continue to monitor and update the Fixed Asset inventory on a perpetual basis throughout the year. Assets should be added when acquired, and updated at all times to reflect their current location and disposition.

The Asset Management Unit shall:

- Coordinate the Annual Fixed Assets Inventory Review; and ensure:
  1) All Sections/Units receive reports of their fixed asset inventory as of June 30th of each year. All Sections/Units must complete this inventory annually;
  2) The Biannual Capital (GAAP/Fixed) Asset Report shall be completed as of December 31st and June 30th of each year; and
  3) All Sections/Units receive reports of their Annual Asset Forfeiture, Technology, and Federal Grant Inventory as of January 31st of each year. All Sections/Units must complete this inventory annually. Assets associated with each of these funding sources shall be accounted for regardless of value.

Subject:	Number:
Asset Management	**ADM-30**

Annual Fixed Assets, Biannual Capital Assets Inventories, Asset Forfeiture, Technology, and Federal Grant Inventories, continued

Whenever there is a change of command at a reporting entity, or a change in the personnel assigned to manage specified fixed assets, an asset inventory shall be completed.

Note: The Asset Management Unit shall be notified before fixed assets are disposed of, so that surplus procedures can be followed.

Exceptions

The following Sections/Units are responsible for the management of their assigned inventory:

- Fleet Section;
- Armorer;
- Traffic Programs (radars, lidars and portable breath test devices);
- Communications Section;
- Special Operations Section/Units; and
- Other Department Section/Units as determined by the Chief Administrative Officer or designee.

Commanding Officers shall maintain a master inventory of their assigned fixed assets that:

- Is accurate and reflects changes as they occur; and
- Includes the valuation of the assets.

These Sections/Units shall also conduct an annual inventory, reconcile their databases, and forward the updated inventory report to the Asset Management Unit as of June 30th of each year.

References: MGL c.7, §4A;
802 CMR 3.00;
Chapter 647 of the Acts of 1989;
MPAC: 17.5.1.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**ADM-34**
Subject:	
Information Technology Resources (ITR)	

Policy

The Department shall regulate the use of Information Technology Resources (ITR), including computers, printers and other peripherals, programs, data, local and wide area networks, and use of the internet.

ITR communications including email messages are considered public records, copies of which may be requested by the public.

Definitions

Department Information Technology Resources: Include computers, printers and other peripherals, programs, data, local and wide area networks, and use of the internet.

User: Any employee and/or contractor of the Department that utilizes any of the above resources.

User Responsibilities

Failure to adhere to this policy may subject employees to disciplinary action, up to and including termination.

Employees assigned to a Department entity where they may have occasion to access another system not owned or supplied by the Department shall comply with the terms and provisions of this policy for all such usage.

Acceptable Uses

All employees are allowed to use ITR to the fullest extent possible for any legitimate law enforcement function.

Unacceptable Uses of Agency ITR

Unless conducting a legitimate law enforcement function, it shall be unacceptable for any employee to use ITR:

- In furtherance of any illegal act, including violation of any criminal or civil laws or regulations;
- For any political or commercial purpose;
- To send threatening, sexual, or harassing messages;

Unacceptable Uses of Agency ITRs, continued

- To access or share obscene, or otherwise inappropriate materials;
- To infringe intellectual property rights;
- To gain, or attempt to gain, unauthorized access to any computer or network;
- For any use that causes interference with or disruption of network users and resources, including distribution of computer viruses or other harmful programs;
- To intercept communications intended for other persons;
- To misrepresent either the Department or a person's role at the Department; or
- To libel or otherwise defame any person.

Supervisor Responsibilities

Supervisors are responsible for ensuring that employees under their command comply with the provisions of this policy and shall monitor use in order to ensure compliance.

Data Confidentiality

Under no circumstances is it permissible for employees or contractors to acquire access to confidential data unless such access is required to perform their job or task.

Under no circumstances may employees or contractors disseminate any confidential information that they have rightful access to unless such dissemination is authorized by proper supervisory authority.

Copyright Protection

Employees shall exercise care and judgment when copying or distributing computer programs or information that could reasonably be expected to be copyrighted.

Hardware or Software Installation

Employees shall not install hardware and/or software on any Department ITR without express written authorization from the Division of Administrative Services.

Computer Viruses

Employees shall exercise reasonable precautions in order to prevent the introduction of a computer virus into the local area or wide area networks. Note that many viruses are spread using email attachments.

Virus scanning software shall be used to check any software downloaded from the internet or obtained from any questionable source. All disks or software shall be inspected for virus infection prior to introduction into the Department system or stand-alone computers or laptops.

Security

Employees shall:

- Change passwords at least every ninety (90) days;
- Never share their passwords with anyone else, unless ordered by proper authority;
- Promptly notify the Division of Administrative Services if they suspect their passwords have been compromised;
- Log off the network or have password-protected screen savers in operation if leaving their ITR unattended for extended periods;
- Not access the internet or other external networks via modem unless they have received prior written permission from the Division of Administrative Services;
- Not move desktop computers, terminals, and printers from their assigned location without written notification and the consent of the Division of Administrative Services; and
- Not transfer to another employee any mobile equipment assigned to the individual such as laptop computers, mobile data terminals, and portable printers without prior written notification from the Division of Administrative Services.

Email

Employees are reminded that email messages are considered public records, copies of which may be requested by any member of the public.

Employees shall:

- Consider email messages to be the equivalent of letters sent on official letterhead and be written in a professional and courteous tone;
- Be aware that emails can be stored, copied, printed, or forwarded by recipients; and
- Not subscribe to email mailing lists, unless related to their job function.

Email shall only be used to communicate official business documents to official recipients. The forwarding of non-business related information is prohibited. Employees who are the recipients of non-business related email are required to discard them and shall not forward them to anyone.

Email attachments that are received from an unknown party should be considered suspicious, and shall not be opened until the sender's identity can be confirmed.

Emails which represent privileged correspondence between Department attorneys and other Department employees shall be clearly marked within the message as "Attorney-Client Privileged." In addition, documents that are sent as attachments to an email shall also be clearly marked "Attorney-Client Privileged."

Subject: Information Technology Resources	Number: ADM-34

No Expectation of Privacy

The Department retains the right to inspect any employee's computer at any time

Use of Department ITR constitutes express consent for the Department to monitor and/or inspect any data that employees create or receive, any messages they send or receive, and any web sites that they have accessed.

Employees shall be aware that network administrators routinely monitor network traffic.

Compliance

Staff Inspections shall conduct periodic inspections of all ITR to ensure compliance with all provisions of this policy.

References

Rules and Regulations;
Executive Order 504 Order Regarding the Security and Confidentiality of Personal Information;
Unit 5A State Police Association of Massachusetts, Article 27;
MPAC: 11.5.1, 41.3.7, 82.1.1.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**ADM-34A**
Subject:	
Social Media/Networking	

Policy

The personal use of social media can have an unintended adverse impact on Department of State Police employees in their official capacity. As such, this policy provides precautionary information as well as prohibitions on the use of social media by Department employees.

When using social media/networking, Department employees (sworn and civilian) should be mindful that their speech becomes part of the worldwide electronic domain.

Department employees should also be mindful to treat Department of State Police business as confidential per Rules and Regulations Article 5.

Official Department Social Media accounts shall be administered by the Office of Media Relations. Maintenance and information posted/contained therein shall be limited to employees authorized by the Colonel/Superintendent and/or the Director of the Office of Media Relations.

Definitions

Networking: An exchange of information or services among individuals, groups, or institutions that may include, but are not limited to: the cultivation of productive relationships for employment or business, networking sites, podcasts, as well as comments posted on a site, message or discussion boards, LinkedIn, Plaxo, Jobster, Craigslist, and MyWorkster.

Post: Content an individual shares on a social media/network site or the act of publishing the content on a site.

Social Media: A form of electronic communication through which users create online communities to share information that may include, but are not limited to: personal messages, videos, photo and video sharing sites, blogs, micro blogging sites, including sites such as Facebook, Twitter, YouTube, Pinterest, Instagram, and Snapchat.

Social Media and Networking: Categories of internet-based resources that integrate user-generated content and user participation. They are online platforms where users can create profiles, share information, and socialize with others professionally, personally, or informally. The interface is conducted through posts or speech via a range of devices such as computers, cellular phones, and tablets to name a few.

Speech: Expression or communication of thoughts or opinions via spoken word, writing, photographs, video footage, or related forms of expressive conduct or communication.

Supervisor Responsibilities

Supervisors are responsible for ensuring that employees under their command comply with the provisions of this policy and address violations as soon as possible.

Responsibilities of Employees

In accordance with Department Policies and Procedures and Rules and Regulations, Department employees using social media/networking applications shall:

- Use appropriate discretion in their reference to the Department and not discredit and/or embarrass themselves or the Department;
- Be aware that speech and/or related activities on social media/networking sites may reflect upon them in their official capacities and/or upon the Department, and act accordingly;
- Be cautioned that speech, on or off-duty, may form the basis for disciplinary action under current law;
- Be aware that privacy settings and social media/networking sites are constantly in flux, and they should never assume that personal information posted on such sites is protected or private;
- Expect that any information created, transmitted, downloaded, exchanged, or discussed in a public online forum may be accessed by the Department at any time without prior notice;
- Not divulge information gained due to their authority; and
- Not make any statements, speeches, appearances, or endorsements, or publish materials that could reasonably be considered to represent the views or positions of the Department without express authorization.

Department Employees should use common sense in all communications, particularly on any social media/networking site. An examination of the facts could potentially result in an internal personnel investigation. Employees are responsible for anything they write or present online. Some examples of prohibited action may include, but not be limited to:

- Speech containing obscene or sexually explicit language, images, or acts and statements, or other forms of speech that ridicule regardless of the intent to malign, disparage, threaten harm or otherwise express bias against any race, gender, religion, or protected class of individuals; and
- Speech involving themselves or other Department personnel reflecting behavior that would reasonably be considered reckless, irresponsible, or unprofessional.

Responsibilities of Employees, continued

Department employees should exercise care if they choose to post personal information on the internet. Some activities in an employee's personal life may impact job performance, the performance of other employees, and/or interests of the Department. Once information is posted, it is potentially accessible by anyone, indefinitely, and such information may result in unintended consequences, such as:

- Limiting future career opportunities (e.g., undercover, covert operations, or attainment of a security clearance);
- Manipulation by defense counsel or civil attorney to undermine or impeach an employee's credibility or integrity in order to hinder a successful prosecution, or to support a lawsuit against the Department or Commonwealth; and
- Being viewed, altered, printed, and redistributed by other internet users including criminal organizations.

Department employees who choose to identify themselves as employees of the Massachusetts State Police whether explicitly, implicitly, or visually shall:

- Be considered to be publicly representing the agency in a professional manner while employed by the Department; and
- Be responsible for all content published on their individual social media site(s).

Creation of Media Application

Colonel/Superintendent shall approve in writing before the creation of any:

- Website, page, fan group or other application of social media using the Department as the basis of such application. Examples may include, but are not limited to:
- Creating a website or fan group dedicated to the Massachusetts State Police;
- Creating an identity using a username such as Massachusetts State Police, MSP, or any term associated with the Department.

Department employees shall **not**:

- Publish Commonwealth or Department intellectual property-protected images using social media without prior approval from the Colonel/Superintendent (e.g., photos of sworn personnel in uniform; marked agency vehicles; videos of training or operations exercises; compilation videos of personnel, vehicles, or equipment; electronic artwork of the State Police patch or seal); and
- Create an identity, website, page, fan group or other application of social media using the Massachusetts State Police as the basis of such a creation without prior approval from the Colonel/Superintendent (e.g., creating a website or fan group dedicated to Massachusetts State Police, using "Massachusetts State Police" or "MSP" in a username).

Subject:	Number:
Social Media/Networking	**ADM-34A**

Violations

Department employees shall notify their immediate supervisor when they become aware of:

- Any personal identifying information of themselves on the internet in violation of this policy; or
- A posting and/or website in violation of the provisions of this policy.

Any sites deemed inappropriate, bringing discredit/embarrassment to the Department and or employees, and/or promoting misconduct whether on or off duty shall be:

- Investigated either through a criminal or administrative investigation.

Investigative Activities

Department employees shall **not**:

- Conduct any activity related to ongoing investigations through their personal social networking accounts.

References

Rules and Regulations, Article 5;
MPAC: 54.1.2.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**ADM-35**

Subject:

Body-Worn and Cruiser-Mounted Cameras

Policy

The Massachusetts State Police (MSP) will implement the use of Body-Worn Cameras (BWC) and Cruiser-Mounted Cameras (CMC) by members to:

- Enhance policing transparency;
- Increase public trust; and
- Help foster police-community relations through public facing recording.

Definitions

Public Facing BWC/CMC Recordings: Are often an effective tool to preserve member and civilian interactions. These recordings are also effective in capturing video and audio evidence for use in criminal and internal investigations, as well as member training. The Department recognizes that video images cannot always show the full account nor do video images capture an entire visual or auditory scene as experienced by the member. For this reason, variations between a member's first-hand account and the BWC/CMC recordings may vary. As such, persons reviewing recordings must be cautious about drawing conclusions about what the recordings actually represent.

Record After the Fact (RATF): Is an audio and/or video only recording feature that may be included in the BWC and the CMC system. RATF captures events that occur while the camera system is powered on, even if not actively recorded by a member. This is a limited ability to retrieve an event that was not originally classified as a recorded event. RATF shall not be enabled unless agreed to by the parties

Purpose

The purpose of this policy is to establish guidelines for the:

- Proper use;
- Management;
- Storage; and
- Retrieval of video and audio data recorded by BWC/CMCs.

It is the policy of the Department to respect the privacy interests of all persons in the Commonwealth, while ensuring professionalism in its workforce.

Note: BWC/CMC footage is subject to the Massachusetts Public Records Law, M.G.L. c. 66, § 10 and, unless the recordings falls within one of the exemptions noted in M.G.L. c. 66, § 10, the Department will release the footage upon request and in compliance with such law.

Training

All Department members shall successfully complete Department-approved training on the operation of the system and this policy.

BWC Activation and Incidents of Use

BWC's shall not be activated remotely by a supervisor.

Members shall activate the BWC in conjunction with official law enforcement duties while:

- On regular tours of duty;
- Overtime assignments; and
- Paid details where such use is appropriate for the proper performance of duties, and where the recordings are consistent with this policy and the law.

If there is an immediate threat to a member's life or safety, making BWC activation impossible or dangerous, the member shall activate the BWC at the first reasonable opportunity to do so when such situation calls for BWC activation. There will be a thirty (30) second buffer for BWC, which means, the thirty (30) seconds prior to activation of the BWC will also be recorded/retrievable as video only.

Every member is required to record contact with civilians, regardless of the number of BWC members present and recording, in the following occurrences:

- Vehicle Stops, motorists assists, and crash investigations;
- Investigative person stops: field interview observations, consensual stops, or articulable reasonable suspicion stops, or stops supported by probable cause;
- All dispatched calls for service involving contact with civilians;
- Initial responses by members, including on-site detentions, investigations pursuant to an arrest, arrests, and initial suspect interviews on scene;
- Traffic safety and sobriety checkpoints, while interacting with the public, and during all field sobriety testing;
- Pat-frisks, searches of persons incident to arrest (if not already activated), consents to search, and inventory searches;
- K-9 searches (applicable to BWC equipped K-9 members only);
- All searches for lost/missing persons or criminal suspects (unless the incident or event is of such duration that deactivating the BWC/CMC is necessary to conserve available recording time pursuant to **BWC/CMC Pause/Deactivation);**
- Incidents of emergency response driving and pursuit driving, however a BWC recording need not be used if Cruiser-Mounted Camera is recording;
- When a member reasonably believes a lawful/peaceful crowd control public event that would not otherwise require recording may transition, or does actually transition, into unlawful activity;
- Any contact that becomes adversarial, including a Use of Force incident; or
- Any other civilian contact or official duty circumstance that the member reasonably believes should be recorded in order to enhance policing transparency, increase public trust and police-community relations, or preserve representations of member-civilian interactions.

BWC members are not required to wear and/or activate BWCs while in a Department

BWC Activation and Incidents of Use, continued

facility, or other areas where general access is restricted; however, booking procedures shall be recorded.

Cruiser-Mounted Camera Activation and Incidents of Use

CMC recordings are video only and may be activated by member-initiated recording or via auto-record trigger. Audio of CMC recordings is provided by the BWC only when the BWC member is present and recording. All CMCs shall be programmed with auto-record triggers after five (5) seconds that will automatically activate recording. These auto-record triggers include activation of emergency lighting, siren use, crash detection, gun rack opening/patrol rifle, and dog door opening, unless the member is in the vicinity of his/her home, in which case the member is permitted to turn off the CMC cameras to avoid the auto-record triggers of gun rack opening/patrol rifle, and dog door opening.

Members may turn off individual CMC camera recordings when the auto-record trigger event does not coincide with a delineated scenario requiring recording. (e.g.: emergency lights are on, but member is working a fixed post assignment).

If the CMC system does not automatically activate by an auto-record trigger when an event recording is required, the member shall activate the device by pressing the "record" button. Members shall utilize the video recording functions of the CMC system whenever it is employed, except where/when exempted by this policy.

There will be a one (1) minute buffer for CMC, which means, the one (1) minute prior to activation of the CMC will also be recorded/retrievable as video only, unless the BWC is activated during that time frame to provide audio. Members failing to record a required incident shall document the circumstances in the applicable report and articulate the reason(s) the incident was not recorded.

Members shall activate the CMC in conjunction with official law enforcement duties while:

- On regular tours of duty;
- Overtime assignments;
- Paid details where such use is appropriate for the proper performance of duties, and where the recordings are consistent with this policy and the law.

If there is an immediate threat to a member's life or safety, making CMC activation impossible or dangerous, the member shall activate the CMC at the first reasonable opportunity to do so when such situation calls for CMC activation.

Every member is required to record contact with civilians regardless of the number of CMC and/or BWC members present and recording, in the following scenarios:

- Traffic and criminal enforcement stops;
- In-progress violations of law;

Cruiser-Mounted Camera Activation and Incidents of Use, continued

- Pursuits;
- Investigative person stops: field interview observations, consensual stops, or articulable reasonable suspicion stops, or stops supported by probable cause including field interviews, interrogations, and field sobriety testing;
- Emergency response driving;
- Escort or motorcade driving;
- Fatal crash or major crime scenes (in accordance with **BWC/CMC Pause/ Deactivation**);
- Safety Cars at traffic safety and sobriety checkpoints, unless otherwise directed by the checkpoint supervisor;
- Prisoner transport, at which time the rear CMC shall be utilized when transporting a prisoner(s) in the rear seat;
- Transport of individuals other than prisoners in the rear seat shall be recorded by the transporting member, unless the passenger is a Department member or other government official;
- Searches of vehicles and/or persons; and
- Any other incident the member deems appropriate while acting in the performance of their official duties.

Notice of Recording

BWC/CMC members shall make every effort to inform civilians that they are being recorded at the earliest opportunity unless there is an immediate threat to the member's life or safety, making BWC/CMC notification impossible or dangerous. BWC/CMC members should make every effort to notify civilians with language such as "Ma'am/Sir, I am advising you that our interaction is being recorded."

For custodial interrogations and crime scenes, BWC members are reminded to comply with the requirements of INV-16 Electronic Recording of Interrogations and crime lab policies, respectively.

Use of a BWC/CMC is an acceptable method of conducting a recording of custodial interrogations and crime scenes.

Consent to Record

BWC/CMC members are not required to obtain consent to record. If a civilian has requested the BWC/CMC member to stop recording, members have no obligation to stop recording if the recording is initiated under any of the circumstances identified in **BWC/CMC Activation and Incidents of Use**. A civilian's request to turn the BWC/CMC off should be recorded, as well as the member's response.

Recording within a Residence

Members recording in a residence shall not record beyond what is necessary for the civilian contact, and not use the BWC with exploratory intent in an effort to create an inventory of items in the residence. BWC/CMC members are not required to obtain consent to record, but must provide notice pursuant to **Notice of Recording**. A civilian's request to turn the BWC/CMC off should be recorded, as well as the member's response.

Recording of Victims / Witnesses

If a BWC/CMC member is in video or audio-recording range of a victim or witness who is giving his/her first account of a crime, the member shall record the encounter with notice to the victim/witness. However, should the member determine the investigation or inquiry would be impeded by continuing to record, or would cause reasons for concern for the safety of the witness or victim, the member has the discretion to turn off the BWC/CMC only as long as necessary to gather the information required to continue the investigation or inquiry. The member shall state the reason for turning off the BWC/CMC prior to doing so.

Audio Only Recording is Prohibited

Intentionally obstructing video recordings while allowing audio only to record on a BWC/CMC device is strictly prohibited. Due to the possibility of violating legitimate privacy expectations, inadvertently recording protected conversations, or unintentionally violating M.G.L. c. 272, §99 Interception of Wire and Oral Communications, all camera pre/post event buffers shall be configured so they do not record audio.

BWC/CMC Pause/ Deactivation

Once the BWC/CMC is activated, recording should continue uninterrupted until or unless the event has paused or concluded. To the extent possible, prior to pausing/deactivating a BWC/CMC, the member should state the reason for doing so.

The following are examples of when an event shall be considered paused or concluded:

- Victim and/or witness contact has paused or concluded;
- All persons stopped have been released or left the scene or an arrestee has arrived at the barracks for booking. If a transporting member has a BWC, recording shall continue until the transporting member arrives inside the station at the booking desk;
- The member determines the investigation or inquiry will be impeded by continuing to record, or would cause reasons for concern for safety of the witness or victim;
- The BWC/CMC member may pause the recordings while consulting with other law enforcement members or supervisors, as such discussions:
    - May be for training purposes; or
    - Could undermine, reveal or disrupt MSP strategy or plans, ongoing investigations; or
    - Could jeopardize the secrecy, safety or security of victims, witnesses, confidential informants, undercover members, sworn members, or members of the public; or
    - For other legitimate law enforcement related reason.

It should be noted that pausing the BWC does not pause the CMC as both systems must be paused independent of each other, but it does stop the audio feed from the BWC;

- The incident has concluded prior to the arrival of the member;
- The incident or event is of such duration that deactivating the BWC/CMC is necessary to conserve available recording time; or
- The member is ordered to turn the BWC/CMC off by a supervisor.

Member Responsibilities for BWCs

At the beginning of each shift, the BWC member shall:

- Ensure that the issued equipment has a charged battery and is functioning properly;
- Notify a Supervisor whenever there is a malfunction or damage to the BWC;
- Shall only use MSP issued and approved BWC technologies; and
- Wear BWC in a manner that does not obstruct or intentionally defeat the purpose of the BWC Policy.

While on duty, the BWC member shall:

- Activate the BWC and record as outlined in the sections above ;
- Properly tag/classify recordings for retention; and
- Document the existence of a BWC recording in written narratives.

If a member fails to properly activate the BWC, fails to record the entire contact, improperly pauses the recording, or the BWC malfunctions, the member should document the circumstances and reason in the incident or arrest report, if known to the member, should an incident or arrest report of the interaction be made. In the event an incident or arrest report was not created, the circumstances and reason for the failure to properly activate should be logged in the Daily Administrative Journal.

Docking/Uploading requirements- BWC Best Practice is as follows:

- Prior to the end of the shift, each member places his/her BWC in his/her docking station. The docking station will charge the BWC's battery and transfer video data to the storage system;
- Each member shall place his/her BWC in a docking station no less than one (1) time per week and upload all of their video data into the evidence management system, unless otherwise directed by his/her Section/Station/Unit Commander;
- The member shall ensure all uploaded videos are properly tagged/classified in the evidence management system for retention;
- Before going on any planned leave of one (1) work week or more, each member shall place his/her BWC in a docking station and upload all of their video data into the evidence management system; and
- If a member becomes aware that this process is not occurring or becomes aware of any other malfunction of the system, the member shall immediately notify his/her first line supervisor.

Member Responsibilities for Cruiser-Mounted Cameras (CMC)

In general, members equipped with CMC systems will follow the same procedures as defined for Body-Worn Cameras.

They shall:

- Ensure the CMC's are in good working order;
- Immediately report any malfunction or damage to a supervisor;
- Activate and record as directed by this policy;
- And upload recordings to the evidence management system upon arriving at any Department station equipped to wirelessly upload CMC video.

Supervisor Responsibilities

The Supervisor of BWC/CMC members shall:

- Ensure all members assigned a BWC/CMC utilize the BWC/CMC in accordance with this policy;
- Upon notification of a malfunction, Supervisors will remove the BWC/CMC from service, report the malfunction or damage to the Management Information Section at 508-820-2690 and issue a spare unit, where available; and
- Access BWC/CMC recordings during the course of duties in accordance with policy's **Internal Access/Review**.

Internal Access/Review

BWC/CMCs and their recordings shall not be used for the purpose of harassing:

- Members of the public;
- Sworn members; or
- Department employees.

BWC members shall be provided, through their unique user name/password, with access to their BWC footage, and may also review that footage prior to making any statements or producing any reports. All members shall also have reasonable access to other Department BWC/CMC footage, and may review that footage, prior to making any statements that could reasonably be seen as resulting in disciplinary action.

In the event a member refuses to make a statement after being provided reasonable access to other Department BWC/CMC recordings, Department administrative action may be taken against the member for the member's refusal to cooperate with an investigation, or to make any statements or reports. In the event a member refuses to make a statement after being denied reasonable access to their own or other Department BWC/CMC recordings, Department administrative action shall not be taken against the member for failing to make a statement, but could still be pursued for the underlying event and/or refusal to cooperate with an investigation.

BWC/CMC Member Access to Footage

BWC/CMC members and other members of the Department may review BWC/CMC recordings as they relate to:

- Their involvement in an incident for the purposes of completing an investigation and preparing official reports. To help ensure accuracy, members are encouraged to review the BWC/CMC recording(s) prior to preparing reports;
- Providing testimony in court to refresh recollection. Members shall inform the prosecuting attorney whether the member reviewed the BWC/CMC recording(s) prior to a court appearance; and
- Providing a statement pursuant to an internal investigation, including member-involved shooting investigations and other critical incidents as outlined in **BWC/CMC Member Access to Footage** Following an Officer-Involved Shooting.

BWC/CMC Member Access to Footage Following an Officer-Involved Shooting

Following an officer-involved shooting, or other use of deadly force, members, including supervisors, shall not view the BWC/CMC recording prior to the Force Investigation Response and Support Team ("FIRST") and/or the State Police Detective Unit (SPDU) of jurisdiction investigating member(s) viewing the recordings and uploading it into the system. This prohibition shall not apply where exigent circumstances exist, such as a member being injured, or where the BWC/CMC recording may reasonably provide identifying suspect information or other pertinent, time-sensitive information that may be valuable in addressing the exigent circumstances in a timely manner.

All members involved in an officer-involved shooting or other use of deadly force, and BWC/CMC members who witness a member-involved shooting or other use of deadly force, shall be authorized to view all BWC/CMC recording(s) prior to a walkthrough and/or statement.

Collecting and Securing BWC/CMC Recordings following an Officer-Involved Shooting or Use of Deadly Force

In the event of an officer-involved shooting or other use of deadly force, FIRST Team personnel and/or SPDU of jurisdiction investigating member(s) shall be responsible for collecting and securing the BWC/CMCs from all involved members and witness members at the earliest opportunity.

FIRST Team personnel and/or the SPDU of jurisdiction investigating member(s) shall ensure that all involved BWC/CMCs are uploaded into the system. Consistent with evidence collection and preservation protocols, BWC/CMC(s) will be returned to member(s) once the BWC/CMC digital files have been uploaded into the system.

Non-BWC/CMC Member Access to Footage

Non-BWC/CMC members who are not supervisors, as defined in **Supervisor Access to Footage**, who wish to access recordings of a BWC/CMC member by:

- Written or verbal permission of a supervisors; or
- In accordance with **Internal Access/Review**, and **BWC/CMC Member Access to Footage Following an Officer-Involved Shooting**, and only if required to produce a report, make a statement, provide testimony, or for training purposes.

Said member shall either submit a verbal or written request via To-From or e-mail with the BWC/CMC member's supervisor. Approval of such request must be documented by the supervisor or Duty Lieutenant in writing via To-From, DAJ entry, or e-mail.

Verbal requests and approvals must be documented in the DAJ by the supervisor or Duty Lieutenant stating the name of the requesting officer, the approving supervisor, and the scope of the request (i.e. BWC/CMC member, date/time of footage…)

Access to Footage

BWC/CMCs and their footage shall not be used for the purpose of harassing members of the public, sworn members, or Department employees.

As part of supervision, any supervisory member within the recording member's immediate

Access to Footage, continued

chain of command shall perform regular reviews and auditing of BWC/CMC usage in accordance with Rules and Regulations Article 3.7 Supervisory Members, and shall not require employee notification. Review of footage for the purposes of evaluations shall not be done outside of the current EES cycle for the member to whom the footage relates.

The Colonel, the Deputy Superintendent, and any Division Commander or his/her designees, in the ranks of Major, Detective Captain, and Captain, may review BWC/CMC recordings for any reason. Any Non-Commissioned or Commissioned Officer conducting a Personnel Investigation may review BWC/CMC recordings pertaining to that investigation.

Any request for access to BWC/CMC recordings outside of the immediate chain of command of the BWC/CMC member, must be submitted in writing via To-From or e-mail to the BWC/CMC member's Division Commander. The Division Commander or his/her designee, as enumerated above, may approve or deny said request in writing. The BWC/CMC member shall be provided written notice of such request if approved.

Nothing in this policy shall be construed to prohibit the Department's Chief Legal Counsel, Legal Division, and Records Unit access to BWC/CMC recordings for legitimate legal purposes such as, but not limited to:

- Public records requests;
- Court orders;
- Litigation;
- Freedom of Information Act requests; and
- Discovery requirements.

The Department and SPAM will make mutually good faith efforts to notify one another if either reasonably anticipates that BWC/CMC footage may be published by any media outlet.

Office of Professional Integrity and Accountability Access to Footage

While mindful that BWC/CMCs and their footage shall not be used for the purpose of harassing members of the public, sworn members, or Department employees, members of the Office of Professional Integrity and Accountability shall conduct periodic reviews to ensure BWCs and CMCs are being used appropriately.

Use of Footage for Training

Both BWC and CMC footage is the property of the Department and may be used by the Department for training purposes. Any member coordinating training may forward a request to the Division of Standards and Training to use BWC/CMC footage for training purposes. Prior to use, involved members shall be notified of intended use of footage and given an opportunity to provide input, including any objections. Final authority for use under this section resides solely with the Colonel.

External Access

BWC/CMC recordings related to an ongoing investigation or in support of a prosecution shall be provided by the State Police Legal Section to the applicable law enforcement entity in accordance with ADM-16 Notifying Prosecuting Agencies Regarding Evidence.

Should a member receive a subpoena for BWC recordings, the member shall direct the subpoena as soon as practicable to the State Police Legal Section.

BWC/CMC recordings are presumptively subject to a public records request (M.G.L. c. 66, § 10). If a member receives a request for BWC/CMC footage from members of the media, the request shall be directed to the Legal Section, with a copy to the Director of the Office of Media Relations. All other requests for BWC/CMC recordings, including victim or witness requests, shall be directed to the Legal Section. Members are reminded of the requirements of Rules and Regulations Article 5.23 Dissemination of Information.

BWC/CMC Recording Retention

No BWC/CMC footage or recordings shall be deleted/destroyed while any related investigation is still open/pending. Similarly, no BWC/CMC footage or recordings shall be destroyed until all appeals and/or related litigation is exhausted and closed. The Department shall retain all other BWC/CMC footage or recordings based on the below retention schedule:

A. Schedule I - Indefinite Retention
- Death Investigation
- Motor Vehicle Accidents Resulting in Death
- Sexual Assault/Abused Person

B. Schedule II - 10 Year Retention:
- Use of Force
- Felony

C. Schedule III - 6 Year Retention
- Misdemeanor

D. Schedule IV – 3 Year Retention
- Motor Vehicle Accidents with Personal Injury
- Investigate Person – member responding to call
- Investigate Premise – member responding to call
- Significant Event - Public Safety
- Traffic Stop
- Member initiated encounter/Field Interview Observation (FIO)

E. Schedule V - 1 year Retention
- Motor Vehicle Accidents with Property Damage only
- No Report - Dispatch / On Site
- Civilian Transport without arrest
- Test/Training

Requests to Delete Video

The camera systems will not allow recordings to be deleted by members. All recordings that do not fall within the retention schedules of **BWC/CMC Recording Retention** shall be retained for 30 days.

In cases in which a recording has been requested for litigation, the District Attorney's Office and/or the Department's Legal Section shall be notified of the request and said request shall be addressed pursuant to evidentiary rules of court.

In the event of a purely accidental activation of the camera system that does not have any relevance to an event requiring camera activation, members may request that the video file be deleted.

Members shall submit an e-mail request with sufficient information to their Troop/Section/Unit Commander who shall review the recording to confirm it is an accidental recording and it contains no footage required for submission as evidence, or that could be subpoenaed for any criminal or civil proceeding.

The Troop/Section/Unit Commander shall submit the request and approval in writing (e-mail is sufficient) to the BWC/CMC System Administrator who shall delete the file and document the reason for deletion and authorizing authority in the audit log.

Video files recorded by members as part of the initial system training sessions may be routinely deleted by the BWC/CMC System Administrator with the approval of the Division Commander of Administrative Services.

Improper Recording

BWC/CMCs shall not be used to record:

- Breaks, meal periods, or time periods when a member is not responding to a call, or when not in service;
- Any personal conversation of or between other department employees without the recorded employee's knowledge;
- Non work-related personal activity, especially in places where a reasonable expectation of privacy exists, such as locker rooms, dressing rooms, or restrooms;
- Investigative briefings and roll calls;
- Encounters with undercover members or confidential informants;
- Departmental meetings, workgroups, in-service training, or assignments of an operational or administrative nature. Using BWC/CMCs for training purposes is not a violation of this restriction;
- Communication with Department members or other law enforcement agency personnel;
- A telephonic conversation, except in accordance with the provisions of State and Federal Law while in the performance of official duties; or
- Strip searches (refer to DET-02 Custodial Inventory).

Improper Use or Dissemination of BWC/CMC Recordings

All recording/footage is the property of the Department, not the employee and any dissemination must be approved by the Colonel or his/her designee, the Legal Section, or be disseminated in the course of their official duties. BWC/CMC recording/recordings shall not be:

- Used for the purposes of ridiculing or embarrassing any employee or person depicted on the recording;
- Randomly reviewed for disciplinary purposes; or
- Copied/filmed/photographed/reproduced in any fashion by any employee other than in the course of their official duties, and with supervisor approval (e.g., using their personal electronic device to copy).

Prosecutorial & Court Ordered Restrictions

Access to BWC/CMC recordings/footage are subject to all state and federal laws, and any orders of a court of competent jurisdiction. BWC/CMC recordings/footage shall be preserved, stored, and retained in accordance with the requests, directions, and orders of appropriate prosecutorial and/or judicial authorities.

BWC/CMC Technological Changes

Vendor technology is constantly changing and vendors routinely add new features to BWC/CMC systems. Only those features approved and accepted by the Colonel/Superintendent shall be utilized for the Department's video systems.

Any additional vendor system features or enhancements shall be vetted by the BWC/CMC System Administrator, and if deemed desirable, shall be presented to the Colonel/Superintendent for approval and bargaining, before implementation.

References

M.G.L. c. 4, §7
M.G.L. c. 66, § 10
Rules and Regulations Article 3.7 Supervisory Members
Rules and Regulations Article 5.23 Dissemination of Information
ADM-16 Notifying Prosecuting Agencies Regarding Evidence
INV-16 Electronic Recording of Interrogations
DET-02 Custodial Inventory
UOF-02 Lethal Force - Response

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**ADM-36**

Subject:

Diversity and Equal Opportunity

Policy

The Department recognizes that when the effects of employment practices, regardless of their intent, discriminate and create adverse impact against any group of people, affirmative action shall be taken to ensure diversity and equal opportunity and provide equitable remedies for the consequences of present and/or past discriminatory practices. This provides a positive benefit by expanding opportunities to society, the public, and all current and future employees.

Purpose

The Department prohibits discrimination in employment on the basis of race, color, religious creed, national origin, ancestry, gender, sexual orientation, protected veteran status, age, and disability.

Strategy for Implementation

The Department shall develop a strategy, which includes plans to address:

- Affirmative action; and
- Diversity and equal opportunity.

The Department, as required and limited by state and federal law, remains committed:

- To ensure equitable participation of minorities, women, Veterans, including Vietnam era Veterans, and persons with disabilities, in all of its operations.

Scope

This policy applies to all employment practices and programs including, but not limited to:

- Recruitment, selection, promotions, termination, transfers, layoffs, compensation, training, and benefits, as well as terms and conditions of employment.

The Department shall annually review, investigate, and when necessary modify:

- The policies relative to facilities and programs accessible to the public; and
- Provisions of reasonable accommodation for persons with disabilities.

Diversity Officer

The Colonel/Superintendent shall appoint a Diversity Officer who shall:

- Develop and implement:
  - An affirmative action plan;
  - A diversity plan; and
  - Track the request, purpose, and dissemination of any protected information.
- Report to the Colonel/Superintendent:
  - Specific goals and timetables for achievement of each plan;
  - The Department's compliance with reporting guidelines and requirements; and
  - Any recommendations regarding equal opportunity.

Divisional Diversity Officer

The Divisional Diversity Officer (DDO) is appointed by the Division Commander and approved by the Colonel and Department Diversity Officer who is the Unit Commander of the Recruitment and Diversity Office.

The DDO shall:

Assist and advise their Division Commander and Unit Commanders in gathering information pertaining to equal employment opportunities specific to their respective Division. This includes:

- Working with the Department Diversity Officer and obtaining Divisional Workforce Demographics; and
- Working to identify and reduce bias within their Division

The DDO will be an informational career path resource for ALL members interested in specific stations, sections or units within their division (For example: AirWing, Marine Unit, VFAS, Gang Unit, K9, SPDU, CINRET, CSSS and CAT Teams etc.).

The DDO will continuously monitor, track, and work with other Divisional Diversity Officers in identifying members who have demonstrated their commitment to the MSP, its organizational values, and who are interested in specific units throughout the State Police. The DDO will contact these members and begin the mentoring process.

Due to the size and complexity of the MSP, DDOs may be provided with assistant DDOs who are approved by the Division Commander.

The DDO is not the avenue for reporting or investigating any external or internal complaint. In these instances, members should continue to follow the procedures outlined in ADM-14 Personnel Investigations and ADM-18 Anti-Harassment/Sexual Harassment and Discrimination.

Responsibilities

The Colonel/Superintendent has the overall responsibility for ensuring equal opportunity and appropriate affirmative action policies exist within the Department. Supervisors at all levels have the responsibility for the successful implementation of the affirmative action and equal opportunity plans.

References

ADM-18 Anti-Harassment/Sexual Harassment and Discrimination;
ADM-14 Personnel Investigations;
Department of State Police Affirmative Action Plan;
Department of State Police Diversity Plan;
Massachusetts General Laws Chapter 151B;
Gubernatorial Executive Orders 237, 240, 390 and 478;
The Equal Pay Act of 1963;
Title VI and Title VII of the Civil Rights Act of 1964;
The Age Discrimination in Employment Act of 1967;
The Equal Employment Opportunity Act of 1972;
The Civil Rights Act of 1991;
Section 504 of the Rehabilitation Act of 1973 ;
The Americans With Disabilities Act of 1990;
The Family and Medical Leave Act of 1993,
Article 1.3.1 Code of Ethics;
Article 2 Organizational Values.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**ADM-41**
Subject:	
Telephone Use/Access	

Policy

This policy defines the proper use of all Department telephones for all forms of communication, including voice, text, multimedia, and native or third-party applications on a cellular telephone. All Department-issued telephones, are intended for official business only.

Within the content of this policy, the term "employees" shall refer to both sworn and civilian Department members.

Department Telephone Use

Department employees shall adhere to Massachusetts General Laws, MSP policies & procedures, rules and regulations, provisions of their applicable collective bargaining agreements and/or the Red Book while utilizing Department telephones.

Department telephones shall not be utilized in a manner that interferes with an employee's official duties and responsibilities. All telephone-related communication shall be conducted in a professional manner, providing appropriate information and assistance to callers, where applicable.

All telephone use, including, but not limited to, voice recordings, call history, text and multimedia messaging, photos, videos, and native or third-party application use, is subject to public records law and litigation-related discovery. In addition, all telephone use is subject to audit and review by the Department.

Cellular telephones shall not be utilized to circumvent radio communications in the ordinary course of Department-related business, except in exigent circumstances or wherein officer safety could otherwise be compromised.

Equipment and Access

Only Department-issued equipment shall be connected to any Department network or telephone jack, or telephone line. Department employees needing nomadic use of a Department-issued telephone number for teleworking or other legitimate business purposes must submit a written request for approval, through appropriate channels, to their Station/Section/Unit supervisor.

Landline Telephone Requests

Requests for additional or deletion of landlines in Department facilities should be submitted in writing by the Commanding Officer of the Station/Section/Unit, through appropriate channels, to the Director of Telecommunications.

Notice of Department Telephone Voice Recording

Department employees are advised that all incoming or outgoing telephone calls from Department facility telephones, including emergency 911 calls transferred from any State Police or local dispatch center, or to any Troop Headquarters or Substation, are subject to audio voice recording.

Telephone Interpreter Services

Department members needing foreign language interpreter services by telephone, for official State Police use, should follow the procedure outlined below:

1. Call Department contracted interpreter service at (833) 254-4575;
2. State the language needed when prompted;
3. State your barracks name (e.g. “SP South Boston”)
   Note: Members not assigned to a specific Troop or Barracks should use “GHQ”;
4. Wait to be connected to an interpreter; and
5. Make an administrative journal entry into RAMS or ACISS indicating the usage of same.

Please note that you do not need a PIN or a code to use this service. The Department’s account is set for Priority Queueing; all incoming calls will be first in line. Also, please note this is for foreign language translation services via telephone only—there is no provision for in-person interpreter services.

Subject:	Number:
Telephone Use/Access	**ADM-41**

Department-Issued Cellular Telephones

Department-issued cellular telephones are restricted to employees or Units whose duties require the use of a cellular telephone to effectively perform the essential functions of the employee's or Unit's job. While-Department-issued cellular telephones are intended to be used for official Department business, employees may make reasonable use of personally assigned Department-issued cellular telephones for personal calls or other use, but may be liable for costs associated with such use.

Requests for Department-issued cellular telephones shall be:

- Submitted through channels, in writing, to the Chief Administrative Officer (CAO).

Employees issued a Department cellular telephone shall:

- Sign for the issued equipment;
- Submit a To-From, through channels, to the CAO and the Fiscal Section if a Department-issued cellular telephone is lost, stolen or damaged; and
- Upon separation from service or transfer from the Department assignment for which the Department issued a cellular telephone, immediately return the cellular telephone to Asset Management or submit a new request, through channels, to the CAO for retention of the Department-issued cellular telephone in his/her new assignment.

Personally-Owned Cellular Telephones

Personally owned cellular telephones should not be used to document evidence. Personally owned cellular telephone records may be subject to litigation discovery if the cellular telephone is utilized to conduct official Department business including, but not limited to, voice recordings, call history, text and multimedia messaging, photos, videos, and native or third-party application use.

The Department is not liable for lost, stolen, or damaged personal cellular telephones or any monetary charges an employee receives while using a personal cellular telephone.

Department employees shall limit, where practicable, personal phone use during work hours or while in view of the public.

References: M.G.L. C. 90, § 13B;
Acts of 2019 Chapter 122 An Act Requiring the Hands-Free Use of Mobile Telephones While Driving;
Massachusetts State Police Training Bulletin 2020-01;
MPAC 81.2.10.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Subject:	Number:
Telephone Use/Access	**ADM-41**

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**ADM-46**
Subject:	
Sexual Activity in Public Places	

Policy

The Commonwealth of Massachusetts has a legitimate enforcement interest in ensuring that sexual activity and/or genital exposures do not occur in public places, where the likelihood of being observed by a casual passerby is reasonably foreseeable.

Disparate enforcement of applicable statutes against any particular group and/or disparate treatment of any group is prohibited.

Definitions

Public Place: For the purposes of this policy only, a place where it is known or reasonably should be known that members of the public may be present and/or may be able to observe activity. An area may be open to the public and not be considered a public place for the purposes of this policy if a reasonable person would not foresee that his/her activity would be seen by a member of the public.

Sexual Conduct: For the purposes of this policy only, the exposure or touching of the genitals, buttocks, or female breasts for purposes of sexual arousal, gratification or offense, or public solicitation to engage in such conduct in a public place. Sexual conduct does not include socializing and expressions of affection absent the particularized conduct described in this subsection.

Criminal Laws

Members shall pay particular attention to the elements of the various offenses when making a determination to arrest possible offenders for engaging in sexual conduct on public property (e.g. rest areas, parks).

All of the elements of a particular offense shall be met in order to charge an individual with an offense.

Most criminal complaints involving consensual sexual conduct on Commonwealth lands generally allege violations of the following Massachusetts General Laws (MGL):

Subject: Sexual Activity in Public Places	Number: ADM-46

Criminal Laws, continued

MGL c. 272, § 16 Open and Gross Lewdness

To sustain a conviction for open and gross lewdness, the Commonwealth must prove five (5) elements:

- That the defendant exposed their genitals, buttocks, or female breasts to one or more persons;
- That they did so intentionally;
- That they did so openly, i.e., with the intent of exposing themselves, or in reckless disregard or substantial risk of public exposure, to others who might be offended by such conduct;
- That defendant's act was done in such a way as to produce alarm or shock; and
- That one or more persons were in fact alarmed or shocked by defendant's exposing their self. Members should identify at least one witness, who is not a police officer, to satisfy this requirement.

MGL c. 272, § 35 Unnatural Acts

The conduct must:

- Occur in a public place;
- Involve oral contact with the genital or anal area, anal intercourse or masturbation of another person; and
- Be done intentionally or with reckless disregard that others may observe the conduct and be offended.

MGL c. 272, § 53 Indecent Exposure and Lewd and Lascivious Behavior

A charge of lewd and lascivious behavior requires both:

- The sexual conduct must occur in a public place; and
- That it be by a person who knows or should know of the presence of another person or persons who may be offended by the conduct.

This section also prohibits the:

- Public solicitation of conduct to be performed in a public place; when
- The conduct committed or solicited involves touching of the genitals, buttocks, or female breasts for the purpose of sexual arousal, gratification, or offense.

Procedure

Members are free to approach and make inquiries to persons in public areas. The approach or inquiry, however, shall neither explicitly nor implicitly assert that persons must respond to their inquiries.

Persons cannot be arrested:

- For failing to respond;
- On mere suspicion;

Subject: Sexual Activity in Public Places	Number: ADM-46

Procedure, continued

- For failing to give an account which satisfies the member; or
- Because of a past offense.

Members shall not order someone to leave a public area in the absence of unlawful conduct.

An investigatory stop or brief detention shall be based on reasonable suspicion.

An arrest shall be based on probable cause.

References

MGL c. 272, § 16;
MGL c. 272, § 53;
MGL c. 272, § 35.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**ADM-47**
Subject:	
Bias-Based Policing	

Policy

The Department of State Police is committed to protecting the constitutional and civil rights of all people.

The Department is committed to bias-free policing.

Sworn Department members are prohibited from engaging in bias-based policing practices.

Sworn Department members shall receive initial training and subsequent annual training in bias-based policing to include its legal aspects and consequences, in order to prevent bias-based policing.

The Department does not endorse, train, teach, support, or condone any type of stereotyping, or bias-based policing, by its members. While recognizing that most members perform their duties in a professional, ethical and impartial manner, the Department is committed to identifying, investigating, and eliminating any instances of bias-based policing.

In conducting law enforcement activities such as criminal investigations, members shall not consider personal characteristics such as race, ethnicity, national origin, gender, gender identity/expression, cultural group, sexual orientation/identity, socio-economic status, religion, immigration status, and/or age, except when credible intelligence relevant to the location and time frame links a person or people of a specific race, ethnicity, cultural group, national origin, gender, gender identity/expression, sexual orientation/identity, socio-economic status, religion, immigration status, and/or age to a specific unlawful incident, incidents, criminal patterns or schemes (suspect specific incidents.)

Except in suspect specific incidents, members are prohibited from considering the race, national origin, ethnicity, sexual orientation/identity, socio-economic status, religion, immigration status, and/or age, gender identity or expression, cultural group, or disability, of members of the public in deciding to detain a person or stop a motor vehicle and in deciding upon the scope or substance of any law enforcement action.

Subject:	Number:
Bias-Based Policing	**ADM-47**

Purpose

Bias practices are unfair, ineffective, promote mistrust, and perpetuate negative and harmful stereotypes.

Allegations of bias-based policing or any other type of discriminatory practice, real or perceived, are detrimental to the relationship between the police officers and the communities they protect and serve, because they strike at the basic foundation of public trust. This trust is essential to effective community-based policing.

Bias-based policing is illegal and an ineffective method of law enforcement. Bias-based policing results in increased safety risks to members and the public and is a misuse of valuable police resources. More importantly, such improper methods violate the civil rights of members of the public and may lead to increased exposure to liability. The Department is committed to an ongoing and open dialogue with community leaders to ensure that it is engaging in bias-free policing. The Department is committed to community policing in all the Commonwealth's cities and towns, and specifically proactively engaging with youth, families and community members to build relationships, solve problems, and prevent crime.

Definitions

Bias-Based Policing: Any prohibited pattern or practice, including, but not limited to, stopping, detaining, questioning, frisking, and searching by police officers, that is based upon a generalized belief that a person of a particular race, ethnicity, national origin, gender, or other characteristic, status, or trait, is more likely to commit certain types of crimes. This type of inappropriate reliance on certain characteristics such as race, ethnicity, national origin, religion, gender, sexual orientation, immigration status, gender identity or expression, economic status, age, cultural group, or disability as the basis for providing differing law enforcement services or enforcement activity as outlined is strictly prohibited.

Suspect Specific Incident: An incident in which a member is lawfully attempting to detain, apprehend, or otherwise be on the lookout for one or more specific suspects who have been identified or described in part by national or ethnic origin, gender, race, religion, sexual orientation, immigration status, gender identity or expression, economic status, age, cultural group, or disability or any other protected characteristic.

Bias-Based Policing Prevention

To prevent bias-based policing, the Department shall:

- Provide training programs to ensure that appropriate employees receive training on bias-based policing practices, implicit bias, the legal aspects and consequences of bias-based policing and implicit bias, and the standards established by this policy;
- Ensure that this policy is disseminated to all members, dispatchers and appropriate civilian employees;
- Continuously review and, where appropriate, revise all procedures that involve the stop, detention, apprehension, or search of

Bias-Based Policing Prevention, continued

individuals to ensure that procedures are in compliance with the provisions of the law and this policy;
- Continuously review performance recognition and evaluation systems, training curricula, policies, and customs of the Department to determine if any practice encourages conduct that may support or lead to bias-based policing; and
- Work with the Executive Office of Public Safety and Security (EOPSS) and the Registry of Motor Vehicles to educate the public on what to expect when either stopped or detained by the State Police, as well as what the officer's expectations are during motor vehicle stops or detainment, to ensure the safety of both officers and the public.

Enforcement of Bias-Based Policing Policy

To enforce the provisions of this policy, the Department shall:
- Take appropriate and timely action to investigate allegations of bias-based policing; and
- Take appropriate and timely measures to correct any institutional practice or policy that may support or lead to the use of bias-based policing.

Responsibilities

Division of Standards and Training shall:
- Promote professionalism throughout the Department;
- Ensure that all employees receive training on the prevention and elimination of bias-based policing;
- Assist supervisors in identifying and modifying potentially problematic behavior;
- Utilize appropriate citizen complaint procedures to document and investigate allegations of bias-based policing;
- Investigate referrals from the EOPSS; and
- Conduct a documented annual administrative review of agency practices including public concerns.

Responsibilities

Position	Duties
Colonel/ Superintendent	Shall: • Promote the Department's commitment to prevent and eliminate bias-based policing; • Ensure all employees receive a copy of this policy; • Ensure all employees comply with this policy; • and • Ensure the continuing analysis and public release of analysis related to documented police interactions with community members.
Supervisors	Shall: • Monitor members conduct to ensure that the standards of this policy are being carried out; • Address instances of non-compliance with this policy; • Ensure that members collect data on race, gender, and searches in accordance with laws, and TRF-08 Citations; and • Take positive steps to identify, prevent, and eliminate any instances of bias-based policing by members of the Department.
Members	Shall: • Provide everyone with fair and impartial bias-free police services consistent with constitutional and statutory mandates; • Respect the diversity and the cultural differences of all people; • Uphold the Department's commitment to lawful and non-discriminatory enforcement that promotes public safety and strengthens the public's trust and confidence; • Promptly report any instances of bias-based policing to a supervisor; and • Take affirmative and positive steps to identify, prevent, and eliminate any instances of bias-based policing by other members.

Subject:	Number:
Bias-Based Policing	**ADM-47**

References: M.G.L. C.12 §11H-2(b);
TRF-08 Citations;
MPAC 41.4.0.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**ADM-49**
Subject:	
Deaf or Hard of Hearing Individuals	

Policy

In accordance with the Americans with Disabilities Act, 42 U.S.C. §12101, *et seq*. (ADA), the Massachusetts State Police is committed to serving all individuals according to their needs. Recognizing that persons who are deaf or hard of hearing have may require auxiliary aids or services to ensure effective communication, the Department recognizes its obligations to provide necessary auxiliary aids or services and is committed to meeting those needs. Individuals who are deaf or hard of hearing are entitled to a level of service equivalent to that provided to other individuals without disabilities.

Definitions

Auxiliary aids and services: Various types of communication aids that assist people who are deaf or hard of hearing to communicate effectively. Examples include qualified interpreters on-site or through video remote interpreting (VRI) services; notetakers; real-time computer-aided transcription services; written materials; exchange of written notes; telephone handset amplifiers; assistive listening devices or systems; telephones compatible with hearing aids; closed caption decoders; open and closed captioning, including real-time captioning; voice, text, and video-based telecommunications products and systems, including text telephones (TTYs), videophones, and captioned telephones, or equally effective telecommunications devices; videotext displays; accessible electronic and information technology; or other effective methods of making aurally delivered information available to individuals who are deaf or hard of hearing.

Deaf or Hard of Hearing: An individual who has or is regarded as having substantially limited hearing with or without assistance within the meaning of the ADA. This includes a person who does not hear well enough to rely on their hearing to process speech and language, even with the assistance of hearing aids

Lip Reading: (also referred to as speech reading): The ability to use information gained from movements of the lips, face, and body to increase understanding. It is important to note that while lip-reading may be effective for some individuals who are deaf or hard of hearing, for many it will be insufficient. Some assessments have

determined that only one third of spoken words can be understood by speech or lip-reading.

Definitions, continued

Qualified Interpreter: An interpreter who, via a video remote interpreting service or an on-site appearance, is able to interpret effectively, accurately, and impartially, both receptively and expressively, using any necessary specialized vocabulary. Qualified interpreters include, for example, sign language interpreters, oral transliterators, and cued-language transliterators.

The Massachusetts Commission for the Deaf and Hard of Hearing (MCDHH) is the state agency that determines who is qualified as an interpreter for MSP.

Sign language: Communication through the use of standardized hand or finger signs or gestures. American Sign Language (ASL) is a form of sign language frequently used in the United States. Signs convey concepts or ideas, even though a sign may stand for a separate English word. Signing individual letters by finger spelling can supplement sign language. Just as there are regional variations (dialects) in spoken English, there are regional differences in sign language.

General Considerations and Guidelines

If a member has any reason to believe that a person who has a need to communicate with the Department is deaf or hard of hearing, the member must advise the person that appropriate auxiliary aids and services, including interpreters, will be provided free of charge when necessary for effective communication. The member will ensure that such aids and services including interpreters are offered, utilized, and documented. Primary consideration will be given to the auxiliary aid requested by the person who is deaf of hard of hearing unless there is another equally effective means of communication available. This means that, upon initiating contact, the member should ask the individual who is deaf or hard of hearing about their preferred method of communication.

Members encountering a person they believe are deaf or hard of hearing should never assume that that the person understands what is being communicated. This caution applies to all forms of communication, whether sign language, speech, writing, or reading.

Communication problems in police-public encounters may result in violations of an individual's civil rights, and provide the potential basis for misunderstandings, problems, frustration, and embarrassment. Therefore, it is important that members are able to

identify when they may be interacting with an individual who is deaf or hard of hearing in order to differentiate the person's actions and demeanor from other causes, and then take appropriate measures to facilitate effective communication.

General Considerations and Guidelines, continued

Some deaf and hard of hearing persons have limited written language skills, particularly involving complex matters such as legal warnings and admonitions. Therefore, members should not assume the effectiveness of this form of communication and should gain confirmation of a person's understanding whenever possible.

Encountering and Communications with Deaf or Hard of Hearing Persons

Deaf persons may attempt to gain the attention of a member by touching him/her when the member is not facing them. This is how deaf and hard of hearing persons commonly gain the attention of others, so that they can see the other person's face and attempt to communicate. Members should not interpret this touching alone as offensive or possibly threatening behavior unless additional factors suggest otherwise.

Members should never assume that the person understands verbal communications until comprehension can be confirmed by appropriate responses to questions or directives. Even where an individual may appear to be comprehending some portion of the communication, verbal communication should not be solely relied upon where an individual has indicated a need for auxiliary aids or services.

Members should not assume that persons who wear hearing aids or cochlear implants (an electronic device that partially restores hearing) can hear and fully understand information that is verbally communicated. Some people use these devices to provide sound awareness rather than to increase speech understanding. Highly stressful situations, background noise, multiple speakers, and complex information and instructions can compromise the effectiveness of hearing aids and cochlear implants. Members can assess comprehension by seeking appropriate responses to simple questions or directives as indicated above.

Once someone is identified as a deaf or hard of hearing person, members should attempt to determine (by written or other forms of communication) the person's preferred means of communication (e.g., sign language, lip reading, reading and note writing, using a laminated communication card, or speech).

Encountering and Communications with Deaf or Hard of Hearing Persons, continued

Deaf or hard of hearing persons may require additional time to respond to commands, instructions, and questions. Members must be alert to indications that a person may be deaf or hard of hearing. Such indications may include, but are not limited to the following:

- The appearance of bumper stickers, rear window decals, or visor notices/symbols indicating the disability;
- Failure of persons to appropriately respond to spoken commands or signals;
- Use of signs, hand signals, or gestures in an attempt to communicate;
- Display of cards by the person noting his or her hearing disability;
- Inability or difficulty of a person to consistently follow verbal instruction or requests for information;
- A need to see the member's face directly, suggesting that the person is attempting to lip read;
- Evidence of assistive devices such as hearing aids, cochlear implants, or picture symbols; and
- Evidence of behaviors that indicate an individual is not receiving effective communication access such as increased agitation or irritability, low frustration levels, withdrawal, or decreased attention.

Members should be cognizant of the fact that some persons who are deaf or hard of hearing may also suffer from inner ear impairments that can affect their balance, or speech may be slurred or otherwise difficult to understand.

Lip Reading

Members attempting to communicate with a person who can lip read should:

- Select a location that minimizes interference and distractions;
- Face the person so that eyes and mouth are clearly visible;
- Stand about three to six feet from the person;
- Avoid excessive body movement;
- Speak only after getting the person's full attention;
- Make questions and instructions short and simple;
- Speak clearly and slightly slower than usual;

- Be prepared to repeat oneself using different words to rephrase any question; and

- Recognize that lip reading is ineffective for most individuals, so be sure to inquire with the individual who is deaf or hard of hearing to determine whether they may need more effective auxiliary aids or services.

Members should address all questions and directives to persons who lip read by facing them directly and speaking in a moderately paced conversational tone.

- Shouting or using exaggerated mouth movements interferes with the ability to lip read.
- Understanding can be further degraded by the presence of facial hair or items in the mouth such as chewing gum, etc.

Sign Language

Generally, members should not rely on family members or friends for sign language interpretation due to their potential emotional involvement, conflict of interest, and legal requirements.

A family member or friend may only be asked to interpret for a deaf individual where there is an urgent need to communicate immediately and that is the only option.

In nonemergency situations, an adult family member or friend may interpret if the deaf person requests that arrangement, the other person agrees, and it is appropriate under the circumstances.

Interpreter Requirements

M.G.L. c. 221, § 92A requires a police department to procure and pay for the services of a qualified interpreter for a deaf or hard of hearing person whenever such person is arrested. The Department will make available access to speech language interpreters as coordinated by the Massachusetts Commission for the Deaf and Hard of Hearing.

Members should be certain that when any deaf or hard of hearing person executes a waiver, such person does so knowingly, intelligently, and voluntarily. In fact, in the case of a waiver of an interpreter, the court must make a special finding that any statement made by such deaf or hard of hearing person was made knowingly, voluntarily, and intelligently.

In simple enforcement situations, such as traffic stops, driver's license checks, or consensual police-public encounters, a notepad and pencil may provide effective communication for any individuals who are deaf or hard of hearing. Members should document the steps they took to provide effective communication with the deaf or hard of hearing individual.

During questioning or interrogation of a suspect in a criminal case, a qualified legal sign language interpreter, including a Certified Deaf Interpreter is almost always required.

Field Resources

Examples of methods in the field that may be sufficient for transactions, such as checking a license or giving directions to a location, or for urgent situations such as responding to a violent crime in progress, may include simple actions such as:

- Hand gestures or visual aids;
- Exchange of written notes or communications;
- Verbal communication with an individual who can lip read by facing the individual and speaking slowly and clearly; and/or
- Use of computer, word processing, personal handheld communication device or similar device to exchange texts or messages.

Arrests

Deaf and hard of hearing people may be subject to arrest like any person without a disability in situations where an officer has the right to make an arrest. Except in cases where arrest is mandated by law, given the complexities associated with the arrest, booking, and housing of a deaf or hard of hearing person, members should consider exercising discretion and utilizing alternatives to arrest that may include, but not be limited to, an application for a criminal complaint instead of making an arrest. This decision will depend on the facts and circumstances of the particular case.

A qualified interpreter need not be available in order for an officer to arrest a subject where probable cause is established independent of interrogating the deaf or hard of hearing suspect.

If probable cause to make an arrest can only be established through questioning or interrogating a deaf or hard of hearing person, a qualified interpreter will be required except in emergency situations.

Some deaf and hard of hearing persons have limited written language skills, particularly involving complex matters such as legal warnings and admonitions. Therefore, members should not assume the effectiveness of this form of communication and should gain confirmation of a person's understanding whenever possible.

All essential communication with the suspect should be completed prior to the application of handcuffs, if possible.

Booking

When booking a deaf or hard of hearing person, members may communicate with the person being booked in order to obtain minimally necessary information required to complete the booking process through the following means:

- Written communications;
- Verbal communications (if possible);
- A companion of the suspect acting as an interpreter, if requested by the suspect;
- A non-certified interpreter; or
- A certified interpreter.

As noted in the “Arrests” section above, some deaf and hard of hearing persons have limited written language skills, particularly involving complex matters such as legal warnings and admonitions.

Rights: A member should advise a deaf or hard of hearing person of his or her rights pursuant to *Miranda* and all other required rights through a qualified interpreter to appropriately ensure that a waiver of those rights is deemed valid by a court.

Subject	Number
Deaf or Hard of Hearing Individuals	**ADM-49**

Booking, continued

Any statements made by a deaf or hard of hearing person, which are elicited without the use of a qualified interpreter, may be challenged in court.

Field Sobriety Testing

Some deaf or hard of hearing persons have reduced verbal communication skills, and/or speech that may be incoherent or otherwise resemble intoxication. These individuals may also have difficulty with equilibrium, which would impact their ability to perform a balance test.

Members administering standardized field sobriety tests should avoid any evidentiary questions during the testing process, as such questions may require an interpreter. Further, if applicable, members must document in their reports these and any other extenuating circumstances that impacted the administration of field sobriety tests.

Interpreter Contact Information

In situations involving the need for an interpreter, a request shall be made through the Massachusetts Commission for the Deaf and Hard of Hearing. The contact information is listed below:

MCDHH – Executive Office
600 Washington Street, 3rd Floor
Phone: (617) 740-1600
Fax: (617) 740-1810
TTY: (617) 740-1700
Videophone: (617) 326-7546
Emergency / After Hours: (800) 249-9949

Online Requests may be submitted at
https://www.mass.gov/how-to/how-to-request-an-asl-interpreter-or-cart-provider

References:

42 U.S.C. §12101, *et seq;*
M.G.L. c. 221, § 92A.

Promulgated By:
John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**DET-01**
Subject:	
Warrant Management	

Policy

Department members shall utilize established warrant management systems in accordance with federal and state laws and regulations and the contents of this policy.

Definitions

Commonwealth's Criminal History Systems Board (CHSB): The state agency responsible for maintaining law enforcement data communications network and systems.

Criminal Justice Information System (CJIS): A computerized system of criminal justice information, available twenty-four (24) hours a day and managed by the CHSB.

Criminal Offender Record Information (CORI): A database of criminal record information where the release is regulated by state and federal laws.

Interstate Identification Index (III): Triple III is an interstate exchange of criminal history record information maintained by the FBI.

Locate: A computer entry that indicates that the wanted person or item has been apprehended or found.

National Crime Information Center (NCIC): Nationwide computerized system of criminal justice information managed by the FBI.

Wanting Police Department (WPD): Primary police agency or Department Station entering a NCIC warrant.

Warrant Management System (WMS): Centralized database operated by the Trial Court of the Commonwealth that provides CJIS users with access to court issued arrest warrants.

CJIS Information

CJIS information shall only be used by law enforcement and criminal justice personnel in the performance of their duties.

Inquiries of a curiosity nature or other types of transactions performed for non-official purposes are strictly prohibited.

Members in the lawful performance of their duties may rely in good faith upon the information received from CJIS and the WMS, and are not liable in any criminal prosecution or civil action for actions based upon said information.

Much of the information in the CJIS computer is codified as CORI, and its dissemination is strictly regulated by law. Employees shall not release information in violation of the CORI laws.

CJIS Representative

Commanding Officers of each Station/Section/Unit containing a CJIS terminal shall:

- Assign a member as the CJIS Representative; and
- Assign a member as the Backup CJIS Representative.

The CJIS Representative shall:

- Act as the liaison to CHSB regarding CJIS training, validation of warrant information, and password oversight;
- Assist other members in the use of the CJIS System;
- Direct members to the CJIS extranet for additional assistance; and
- Ensure all members are informed of updates, publications, or modifications to the CJIS network.

Warrant Databases

CJIS warrant information may be found in:

- WMS which contains most of the state warrants entered after 1995;
- CJIS/NCIC which contains information on federal, state, and nationwide warrants entered prior to 1995, including in-state parole warrants; and
- The Board of Probation (BOP) record query of an individual that may indicate a default from a court appearance.

A warrant on the WMS shall constitute notice and the printout of the warrant represents a true copy.

CJIS Inquiries

The Desk Officer or Dispatcher shall be aware that a WMS inquiry which yields a hit shall be considered probable cause to arrest when the warrant does not indicate recall or locate.

The Desk Officer or Dispatcher shall:
- Verify the warrant hit in CJIS/WMS; and
- Contact the court of issue if the warrant cannot be located.

The Desk Officer or Dispatcher, when notified that a person has been arrested on a WMS warrant, shall:
- Place a locate against all CJIS wanted records to indicate that the wanted person has been apprehended; and
- Print a copy of the warrant.

The arresting member shall:
- Give a true copy of the warrant to a detainee who requests a copy within six (6) hours.

If the detainee is subsequently released on bail, the arresting member or designee shall:
- Remove any WMS warrants from the WMS system for which the detainee had been taken into custody; and
- Place a copy of the Recall Notice with the detainee's personal property prior to the detainee's release.

Court Information for WMS

Members making a request for a WMS warrant shall provide a completed warrant application to the court of jurisdiction.

The clerk from the court of jurisdiction is responsible for the entering, recall, and removal of WMS warrants from the system.

NCIC Warrants

WMS warrants do not automatically enter into NCIC. The Department shall enter NCIC warrants in order to provide out of state access or rendition even when the warrant is located within WMS.

Any felony or serious misdemeanor warrant may be entered:
- When the District Attorney has authorized rendition; and/or
- For officer safety, licensing, or employment, providing the opening notation in the remarks field is no extradition/rendition (NOEX).

All warrants entered into NCIC shall be in conformance with CJIS/NCIC and Department policy.

NCIC Warrants, continued

NCIC/NOEX warrants entered and maintained by Department entities shall be checked by designated personnel:

- Weekly for recall notices from the courts; and
- Quarterly during the months of January, April, July and October for accuracy and compliance.

NCIC/NOEX warrant file folders shall be kept and maintained by Troop Headquarters or the station of entry as the WPD, and shall contain:

- A copy of the WMS warrant;
- Driver's license information;
- Missing and wanted checks;
- A copy of BOP and Triple III records; and
- Any other pertinent information.

CJIS or NCIC Warrant Confirmation

A CJIS (non WMS) or NCIC warrant that yields a hit shall not be probable cause to arrest. However, once the warrant is confirmed as active with the entering agency there may be probable cause to arrest.

When the Department receives a hit from CJIS and/or NCIC, an immediate confirmation with the agency that originated the record in the system shall be made before an arrest or seizure is made.

The Desk Officer/Dispatcher shall:

- Contact the agency that originated the record in the system by telephone to confirm the warrant; and
- Confirm the warrant following CJIS procedures.

When a request for confirmation is made for CJIS/NCIC warrants held by the Department, the Desk Officer/Dispatcher shall:

- Locate the original warrant and confirm the information following CJIS procedures ensuring the response back to the requesting agency is performed within:
  - Ten (10) minutes for an urgent request; or
  - One (1) hour for a routine request; or
- Cancel the warrant.

CJIS Responsibilities

Members who use the CJIS network are responsible for:

- Familiarizing themselves with the CJIS and NCIC operating manuals; and
- Maintaining bi-annual CJIS certification.

The name and Department identification (ID) number of the person requesting a BOP or Triple III shall be indicated in the "Requested by" or "Attention" fields.

Subject: Warrant Management	Number: DET-01

Justification for BOP / Triple III Checks

Members shall only conduct BOP checks for:

- A history of violence and weapons charges to be disseminated immediately for officer safety;
- An investigation;
- Subjects under arrest; and/or
- Background checks for a legitimate law enforcement purpose.

Members shall only conduct Triple III checks for:

- Legitimate law enforcement purpose;
- Background check for a person applying for employment; and/or
- Background check of a person applying for a Firearms Identification card, or a License to Carry Firearms Permit.

References: MGL c.276, § 11-20, § 23A, § 29;
MGL c.248, § 26;
MGL c.22C, § 10;
MGL c.6, § 167-178;
MPAC: 1.2.5, 74.1.3, 74.3.1.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**DET-01A**
Subject:	
Warrants, Summons, or Subpoenas	

Policy

In furtherance of a legitimate law enforcement purpose, members shall serve warrants, summons, or subpoenas once they become aware of their existence, or as otherwise ordered.

Definitions

Default Warrant: After being given proper notice, a person fails to appear in Court.

Governor's Warrant: When a person arrested outside of Massachusetts has an active warrant in Massachusetts, the District Attorney's Office/Attorney General's Office requests they be returned to Massachusetts through a Governor's Warrant.

Straight Warrant: When an officer, instead of requesting a summons, requests a person be arrested for a crime. Also, if a person fails to report to their Probation Officer, the Probation Officer may ask the Judge for a Straight Warrant.

Default Warrants and Bail

Type of Default Warrant	Bail
Felony or misdemeanor punishable by imprisonment for more than one-hundred (100) days.	Only by a judge of the court that issued the warrant or the court of jurisdiction holding the warrant.
Misdemeanors punishable by imprisonment for one-hundred (100) days or less.	By any person authorized to admit bail.

A detainee arrested on a default warrant, who is not released on bail, shall be:

- Transported to the court of jurisdiction where the arrest was made; or
- Transported to the court that issued the warrant.

Straight Warrants

An individual arrested on a straight warrant shall be transported to the barracks of jurisdiction for booking and processing.

Governor's Warrants

Whenever the Department receives notification that a person wanted by the Department has been arrested in another state as a fugitive from justice:

Step	Action
1	The Desk Officer receiving such information shall contact the Troop Duty Officer who shall contact the Detective Unit of jurisdiction.
2	If the District Attorney authorizes the rendition of the detainee named in the warrant, the Commanding Officer of the Detective Unit of jurisdiction shall: • Notify the arresting out-of-state agency of the decision by telephone and CJIS Fox Messenger as soon as possible.

Whenever the Department receives a Governor's Warrant from another state, it shall be forwarded to the Commander of the Detective Unit of jurisdiction.

The Detective Unit Commander shall:

- Execute the warrant by proper means; and
- Ensure all legal requirements are adhered to.

Service of Summons/ Subpoena

The service of a summons or subpoena shall be logged by the Desk Officer in the Daily Administrative Journal and shall include:

- BOP check for member's safety;
- Date and time service was executed or attempted;
- Name of member executing or attempting service;
- Name and address of person on whom legal process was served or executed;
- Method of service or reason for non-service; and
- Address of service/attempt.

Whenever possible, the summons/subpoena shall be served by giving a copy, in hand, to the party named.

If the party is not home when the service is attempted, the summons/ subpoena:

- May be left with another responsible person residing at the residence; or
- May be left at the last place of abode of the person named.

If the person lives outside the area where service can be made, and there is sufficient time, the summons/subpoena may be mailed to the last known address.

If the summons/subpoena is for a juvenile, service may be made in hand to the parent or guardian of the juvenile.

Subject:	Number:
Warrants, Summons, or Subpoenas	**DET-01A**

Service of Summons/ Subpoena, continued.

If the service of the summons/subpoena is not possible, it shall be returned to the court of issuance, with a reasonable explanation for non-service.

References: MGL c.276, § 11-20, § 23A, § 29;
MGL c.248, § 26;
MGL c.22C, § 10;
MGL c.6, § 167-178;
MPAC: 1.2.5, 74.1.2, 74.2.1, 74.3.1.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**DET-02**
Subject:	
Custodial Inventory	

Policy

Any person (detainee) who comes into the custody of the Department shall be searched.

Purpose

- To protect members and detainees from harmful items or substances that may have been concealed by the subject;
- To protect members from claims of lost, stolen, or damaged property; and
- To establish and define the processing of detainees who come under the care and custody of the Department.

Inventory Protocol

Members are authorized to:

- Search a detainee and remove any property from their clothing or person;
- Search the contents of any outer garments, bags or accessories; and
- Read or examine documents, papers or other records only to the extent necessary for custodial purposes, to include ascertaining or confirming a detainee's identity, and/or ensuring a detainee's physical well-being.

Members SHALL <u>NOT</u>:

- Physically search a detainee for the sole purpose of determining the detainee's gender; and/or
- Use custodial inventory searches as a pretext for an investigative search.

Members SHALL:

- Conduct searches of transgender or intersex detainees in a respectful and appropriate manner and in the least intrusive manner possible, consistent with security needs.

Inventory Protocol, continued

Members searching a detainee shall:

- Inventory any documents, currency, jewelry, or valuable items found, carried or concealed by the subject;
- Record inventory on the SP 2 Custodial Property Inventory;
- If possible, inventory items in the presence of the detainee;
- Have the booking member and the detainee sign the SP 2 Custodial Property Inventory. If the detainee refuses to sign, note the refusal and the reason, if any; and
- Properly secure the detainee's property in a locked container. Any items that cannot fit into the locked containers normally used for detainee property shall be properly secured within the Temporary Evidence/Contraband/Property (ECP) locker. If a key is used to lock the property container, the key will be secured properly to prevent unauthorized access.

Member conducting the booking shall, before placing the detainee in a cell:

- Have the detainee remove
  - Loose or extraneous clothing ;
  - Shoes, belts, ties;
  - Jewelry, necklaces, neck chains; and
  - Any other article that the detainee may use to escape or cause harm to themselves or others.
- Scan the detainee with a hand-held metal detector.

The following items may be retained by a subject in the cell, unless a member believes it would create a hazard:

- Wedding ring;
- Currency;
- Eye glasses, hearing aids; and
- Prosthesis – which should be searched if practicable.

Valuable Property, Currency and Jewelry

The member searching a detainee that has valuable property, currency or jewelry shall:

- Record the items on the SP 2 Custodial Property Inventory;
- Document contraband and/or any confiscated property in the related Incident Report;
- Count currency by denomination and verify amount with a witnessing member present;
- Package and seal valuable property, currency or jewelry in a Department evidence bag (evidence bags shall be labelled: 1 of 1, 1 of 2, 2 of 2, accordingly), and initial the seal;
- Secure valuable property, currency or jewelry within a secure/locked container within the appropriate detainee belongings area while the detainee remains in Department custody; and

Valuable Property, Currency and Jewelry, continued

- Provide the Desk Officer with a copy of the investigative report and SP-2 Custodial Property Inventory. The Desk Officer will insure that detainee's valuable property, currency or jewelry was inventoried and secured, and record the member who inventoried and secured these items.

If a detainee leaves the Department's custody, or is transported or transferred to another facility, and the detainee's valuable property, currency or jewelry is not returned, the Desk Officer shall immediately:

- Secure the valuable property, currency or jewelry within the Temporary ECP Locker;
- Log the valuable property, currency or jewelry within the Temporary ECP Journal;
- Make a log note into the DAJ of the time the valuable property, currency or jewelry was placed into the Temporary ECP Locker;
- Notify the Troop Duty Officer; and
- Provide a copy of the investigative report to the ECP Custodian or Assistant ECP Custodian to be placed with the valuable property, currency or jewelry until the owner returns to collect property.

The Arresting Member shall:

- Make every effort to return the valuable property, currency or jewelry to the owner, or to a designated person identified by the owner, when the owner fails or cannot return to the Department to collect such property.

Return of Property

When the detainee is released from custody, their property (except seized property) shall be returned to them and:

- The detainee shall sign the SP 2 Custodial Property Inventory acknowledging the return; and
- If the detainee refuses to sign the form, the refusal and the reason, if any, shall be recorded.

If the detainee is to be transported or transferred to another facility, the transporting/transferring member shall ensure that:

- A copy of the SP 2 Custodial Property Inventory has been provided to the facility and/or the personnel taking custody of the detainee;
- The name of the person taking custody is recorded on the original SP 2 Custodial Property Inventory;
- The person taking custody has signed the SP 2 Custodial Property Inventory; and

Return of Property, continued

- The original SP 2 Custodial Property Inventory is returned to the Department facility where the detainee's inventory search was conducted.

Valuable property, currency or jewelry stored with the ECP Custodian or Assistant ECP shall:

- Be returned to the owner on a mutually agreed upon time and date.

Container Protocols

Any closed unlocked container shall be opened and each article inventoried individually.

If a container is locked and secured, or if a container cannot be opened without damaging it, the member shall ask the detainee for consent to open it.

If consent is not given, the member shall not open the container unless:

- Probable cause exists to believe that the locked container shall put the member or others in immediate risk of injury or loss of life.

If the container is not opened, it shall be inventoried as a single unit.

A member shall apply for a search warrant to open a locked container if they have probable cause to believe the container has inside it:

- Fruits or instrumentalities of a crime; and/or
- Evidence, contraband or weapons.

Strip Search Protocols

A strip search entails:

- Any search of a detainee requiring them to remove or rearrange some or all of their clothing to permit the visual inspection of skin surfaces, specifically the buttocks, genital/groin area, and/or breasts; so that a visual inspection can be made of all areas of the detainee's body where weapons, dangerous instrumentalities, evidence, or contraband may be concealed.

The need for a strip search is based upon:

- The particular circumstances surrounding the arrest, as well as probable cause to believe the detainee possesses contraband or weapons that may jeopardize the health and/or safety of the detainee and/or those who may come into contact with the detainee.

Strip Search Protocols, continued

The search shall be documented in the arrest report and include the following information:

- Individual searched;
- Justification for performing the search;
- Supervisor providing approval or exigency warranting search;
- Member directing and conducting strip search;
- Other individuals present during search, both members and civilians;
- Location of search, including steps taken to protect privacy; and
- Items of contraband, if found.

Strip searches shall only be conducted:

- With the approval of a supervisor, unless exigent circumstances exist;
- Whenever practicable, by two (2) members of the same gender identification as the detainee. If the detainee is an Intersex Individual or Gender Non-Conforming Male or Gender Non-Conforming Female, refer to DET-08 Gender Identity and Expression;
- In an area that affords complete privacy (strip searches shall not be conducted outside of a Department facility unless exigent circumstances exist);
- Out of the public view (including video cameras, windows, etc.);
- Without any touching of the detainee (although the detainee may be asked to bend at the waist and spread their buttocks);
- In a reasonable, non-abusive, and professional manner; and
- Only for the duration necessary to complete the search.

Various other factors may be considered while conducting the search, including, but not limited to, the age (e.g. status as a juvenile) and mental capacity of the detainee.

Members assigned Body Worn Cameras (BWC) conducting or present during a strip search shall follow the mandates of ADM-35 Body-Worn and Cruiser-Mounted Cameras and deactivate the BWC.

Body Cavity Search Protocols

Members shall not conduct visual searches or physical intrusions into body cavities.

A body cavity search is:

- A search conducted pursuant to a warrant, issued by a judge, that is based on a strong showing of particularized need supported by a high degree of probable cause; that
- Authorizes a medical professional to conduct an internal manual inspection of any human body cavity.

Body Cavity Search Protocols, continued

A member or supervisor seeking such a warrant must:

- Show a **high degree of probable cause** that the detainee has contraband or weapons hidden in a body cavity that may jeopardize the health and safety of the detainee and/or anyone with whom the detainee may come in contact.

Body cavity searches shall only be performed:

- By a medical practitioner in appropriate medical surroundings; and
- Pursuant to a search warrant issued by a judge that authorizes a body cavity search.

Other factors to consider include the age (e.g. status as a juvenile) and mental capacity of the detainee.

Members assigned Body Worn Cameras (BWC) present during a body cavity search shall deactivate the BWC.

The warrant requirement shall apply:

- Where an item may be viewed partially protruding from a body cavity.

No warrant is required when:

- A detainee voluntarily and personally extracts any item from their own body cavity; and
- Cases involving exigent circumstances where medical personnel perform an operation, necessitated solely by good medical practice for medical reasons, which incidentally results in the recovery of evidence for police use.

The body cavity search shall be detailed and documented in the arrest report in addition to any other court reporting requirements.

References: SP-2 Custodial Property Inventory;
Commonwealth v. Sullo, 26 Mass. App. Ct. 766,768 (1989);
Commonwealth v. Thomas, 429 Mass. 403 (1999);
Rodriques v. Furtado, 410 Mass. 878 (1991);
ADM-35 Body-Worn and Cruiser-Mounted Cameras;
DET-08 Gender Identity and Expression;
MPAC: 1.2.8, 1.2.4, 72.5.1.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**DET-03**
Subject:	
Detainee Transportation	

Policy

Safety is the paramount concern when transporting detainees. Members shall always keep in mind:

- The safety and well-being of themselves and others;
- The proper restraint of the detainee to prevent escape or injuries;
- The detainee's safety and rights; and
- Members transporting detainee(s) that pose a security risk or identify/exhibit a medical risk shall notify the desk officer prior to arrival at the barracks.

The transfer of custody from point of arrest to the facility receiving the detainee (eg: barracks, court, other facility…) shall be documented in the DAJ.

Detainee Search Protocols

Cruisers shall be searched before and after transporting detainees for contraband, weapons, fruits or instrumentalities of a crime, and/or evidence. A search is also part of the routine cruiser inspection at the beginning of the shift.

All detainees shall be searched for weapons and contraband prior to being placed in a cruiser or whenever transported. For searches involving an Intersex Individual or Gender Non-Conforming Individual, refer to DET-08 Gender Identity and Expression. Never assume that someone else has searched a detainee.

Under exigent circumstances, it may be necessary for a member to search a detainee of the opposite gender. Such a search shall be conducted professionally and be limited to the minimal invasion of privacy necessary. In other situations it may be more prudent to request assistance by an officer of the same gender as the detainee, or conduct the search in the presence of others.

Cruisers

Cruisers which are routinely used to transport detainees shall have:

- Safety barriers (detainee cages);
- The rear passenger compartment windows and locks disabled;
- Rear passenger seat belts; and
- Rear passenger door locks that cannot be unlocked from the rear passenger compartment.

When transporting a detainee, members should not respond to calls for service unless:

Cruisers, continued

- The situation clearly poses a serious risk to others; and
- The risk to the detainee is minimal.

Interruption of transporting a detainee shall be limited to circumstances that require the immediate intervention of a member, e.g. personal injury crash. Any interruption of the transport of a detainee shall be reported to and recorded by the Desk Officer of jurisdiction including the specific location and cause for the interruption of transport.

In the event a detainee is transported a longer distance, such as an extradition, only those stops required for fuel, food or personal necessity shall be made. The detainee shall be under the direct supervision of at least one member during such stops.

Detainee Restraint Protocols

Unless extenuating circumstances dictate otherwise, members transporting detainees:

- Will ensure detainees are handcuffed with their hands behind their back;
- Will use alternate methods when physically unable to handcuff someone behind their back; and
- Double lock handcuffs to prevent inadvertent tightening or to avoid causing or aggravating any injuries.

If detainees are to be transported for an extended period, members may handcuff them in front. Members may also use a waist chain to secure the hands to the waist if the member has been trained by the Department on use of a waist chain.

Detainees should not be handcuffed or restrained to any part of the vehicle (except for use of the seat belt).

Alternate detainee restraint devices shall be used only when authorized by the Department and the member applying said restraint device has received training from the Department.

Seating Positions

Members shall:

- Ensure that detainees being transported are visually observable at all times;
- Secure detainees with a seat belt;
- Not transport more than two (2) detainees at a time, unless authorized by a supervisor;
- Not transport two (2) detainees in a cruiser without a safety barrier, unless another member is present;
- Whenever practical, transport detainees of the opposite gender in separate vehicles; and
- Ensure detainees of opposite gender are not transported to court in the same vehicle pursuant to Massachusetts General Laws (MGL) c.276, § 53.

Seating Positions, continued

IF the cruiser has...	Then, unless circumstances dictate otherwise, detainee(s) should be placed...
A safety barrier.	In the rear compartment, using the right seat first.
One (1) officer, one (1) detainee, no safety barrier.	In the right front seat.

IF the cruiser has...	Then, unless circumstances dictate otherwise, detainee(s) should be placed...
Two (2) members, one (1) detainee, no safety barrier.	In the right front seat with the other member behind them.
Two (2) members, two (2) detainees, no safety barrier.	One in the right front, one in the right rear seats, with the other member seated behind the driver.

Transportation of Juveniles

Juveniles shall not be transported:

- With adult detainees; or
- To court or other institutions in a "patrol wagon" as stipulated in MGL c.119, § 34.

Transporting Opposite Gender Detainees

Members transporting detainees of the opposite gender shall radio their Station/Unit Desk Officer, and have a Daily Administrative Journal (DAJ) entry made of the:

- Location;
- The number and gender of their detainee(s);
- Preliminary charges against the detainee(s);
- Intended destination;
- Beginning odometer mileage, and upon arrival, the ending mileage; and
- If necessary, request for back-up.

When transporting an individual of the opposite gender, refer to DET-08 Gender Identity and Expression.

Communication

Conversations with detainees shall be professional and kept to a minimum.

- Conversations between detainees shall be limited by the transporting officer for safety reasons.

Members will not allow detainees to use communications equipment while in transport, nor stop to allow a detainee access to communication equipment.

Protocols for Transferring Prisoners

When transporting a detainee to or from another agency or a court detention facility, members shall:

- Secure firearms if required by that facility's protocol;

Protocols for Transferring Prisoners, continued

- Remove restraining devices in the designated area at the direction of the receiving agency, when and if deemed safe to do so, by the transporting member;
- Positively identify the detainee by ID, photographs or fingerprints;
- Deliver or receive the necessary documentation, paperwork, and/or information, including any arrest reports or other written reports documenting why the detainee was taken into custody, copies of any warrants, and any documents used for identification or related to any medical condition, flight risk, suicide risk, safety risks or any other condition that the receiving agency or court should be aware of concerning the detainee;
- Document the transfer of custody in the DAJ; and
- Adhere to procedures within DET-02 Custodial Inventory regarding detainee's property.

If the detainee is a security hazard, suicide risk, or has a condition that the receiving agency or court should be aware of, the receiving agency shall be advised in writing of that condition. This written notification will be included with other necessary documentation that accompanies the detainee. A copy of this written notification will also be placed and retained with the written incident report.

Medical Considerations

While in transit, if a detainee notifies the transporting member of an illness or injury, and if in the member's opinion an illness or injury exists and requires immediate attention, the member shall transport the detainee to the nearest medical facility for an examination.

- The transporting member shall notify the Desk Officer;
- The Desk Officer shall notify the medical facility of the particulars prior to the detainee's arrival; and
- The transporting member will exercise caution and closely monitor the detainee at all times if it is necessary to remove the detainee's restraints during treatment at the medical facility. Upon arrival, the member shall adhere to the procedure outlined in DET-06 Detainee Monitoring.

If a detainee is admitted to a medical facility, the Department shall provide, or ensure proper security arrangements, or arrange for the detainee to be bailed.

If released by the medical facility, the detainee shall be transported to the nearest barracks or facility, as appropriate. When released, the detainee's condition shall be recorded in the DAJ. All instructions for future treatment and medication should be obtained in writing, signed by the attending physician and placed with the detainee's property.

Medical Considerations, continued

If, in the member's opinion, the detainee's reported or observable illness or injury does not require immediate attention while in transit, then upon arrival at the booking location, the member will adhere to the procedures outlined in DET-06 Detainee Monitoring.

When transporting a physically or mentally challenged detainee, special care and attention may be required. The transporting member should use discretion as to the type of restraints or type of vehicle to be used, and the Troop Duty Officer shall be notified.

Special Situations

No detainee or individual in custody shall be allowed to participate in any operation and/or function without the specific written approval of the Division Commander.

Section/Units that conduct such operations or functions on a regular basis may request blanket authorization from their Division Commander. If such authorization is granted:

- Sufficient security shall be deployed to maintain control of the detainee or individual;
- The intended destination shall be inspected in advance by a member;
- Control of the perimeter shall be maintained;
- There shall be minimal contact between the detainee and others; and
- Any other measures deemed necessary by the officer-in-charge (OIC) shall be taken.

Detainee Escape Protocols

Position	Duties
Transporting Member	• Immediately notify the appropriate Desk Officer of: o Cruiser number, member's name, rank; o Exact location; o Detainee method of escape, escape route, and means of transportation; o Name and aliases of escapee, and a physical description including clothing; and o Criminal history and safety risk of the escapee, and the pending charges; and • Immediately make every attempt to recapture the escapee, and if unable to do so, preserve the scene for tracking dogs and investigators; and • Include the details of the escape and recapture efforts in an incident report.
Desk Officer	• Immediately notify the Troop Duty Officer of jurisdiction; • Notify all patrols and local departments of the escape; and • Make the appropriate DAJ entries.

Detainee Escape Protocols, continued

Position	Duties
Troop Duty Officer	• Immediately request K-9, Air Wing and other tactical resources as deemed necessary; • Dispatch a supervisor to the scene to: o Assume control of the recapture operation; o Investigate the circumstances of the escape; and o Prepare a report with findings and recommendations; and • Notify: o State Police Detective Unit of jurisdiction; and o The Troop Commander.
Troop Commander	• Notify Division Commander; • Administratively review report(s) for further action; and • Take actions to prevent reoccurrences.

Commercial Air Transportation and Armed Members

Members shall be certified and follow the federal Transportation Security Administration (TSA) guidelines and Code of Federal Regulations (CFR) Title 49 Carriage of Weapons by Law Enforcement Officers.

Troop/Section Commanders shall ensure the following protocols are followed when members, under their command, fly on commercial airlines while armed.

- An administrative message shall be sent to the Transportation Security Administration (TSA) by the GHQ Communications Section via the National Law Enforcement Telecommunications System (NLETS), requesting a unique alphanumeric identifier receipt for the member who will be flying armed;
- The member shall carry the receipt containing all the pertinent information required by TSA to be verified at the airport on the day(s) of travel; and
- The member shall also carry the appropriate number of signed original Letters of Authority from their Troop/Section Commander and surrender a letter to the airline carrier(s) when requested.

Commercial Air Transportation and Armed Members, continued

- The Letters of Authority shall be on Department letterhead and shall include:
  - The name(s) of the member(s);
  - The dates and itinerary for fights;
  - Certification that the member(s) have completed the TSA's Law Enforcement Officers Flying Armed Program;
  - The circumstances for the need to carry a firearm; and
  - The original signature of their Troop/Section Commander and a contact number for verification.

Note: Failure to provide the unique alphanumeric identifier may result in delays due to the additional verification requirements. The airline and the pilot have the discretion to refuse armed members on any flight.

Procedure Transporting Prisoners by Commercial Airlines

When transporting a detainee on an commercial airline flight, members shall:

- Notify TSA and the airline of the name(s) of the detainee(s) and the accompanying member(s) at least one (1) hour before the flight;
- Notify TSA and the airline if the detainee is considered a "high risk" at least twenty-four (24) hours, or as soon as possible, before the scheduled departure. If so, at least two (2) members shall escort the detainee and arrive at the check-in counter at least one (1) hour before the flight. Only one dangerous detainee is allowed on the same flight;
- Ask to board the plane first, and deplane last;
- Sit in the rear of the plane, maintaining one (1) member between the detainee and the aisle;
- Ensure that no food, utensils, or items be given directly to the detainee without checking the items first; and
- Not consume, nor allow the detainee to consume, alcoholic beverages.
- **Note:** There shall always be at least one (1) member per detainee. At least one (1) member shall be the same gender identification as the detainee. If the detainee is an Intersex Individual or Gender Non-Conforming Male or Gender Non-Conforming Female, refer to DET-08 Gender Identity and Expression.

Members shall carry:

- Department issued badge and identification card;
- A secondary valid government issued ID;
- Necessary boarding paperwork;
- Letters of Authority to travel while armed on commercial flight; and
- Adequate restraining devices.

Subject:	Number:
Detainee Transportation	**DET-03**

References: DET-02 Custodial Inventory;
DET-06 Detainee Monitoring;
DET-08 Gender Identity and Expression;
MGL c.276, § 53;
MGL c.119, § 34;
Code of Federal Regulations (CFR) Title 49 Transportation;
Transportation Security Administration (TSA) "Law Enforcement Officers Flying Armed" Program;
MPAC: 70.1.1, 70.1.2, 70.1.3, 70.1.4, 70.1.5, 70.1.6, 70.1.7, 70.2.1, 70.3.1, 70.3.2, 70.4.1, 70.4.2, 70.5.1.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**DET-04**
Subject:	
Holding Facility Design and Inspection	

Policy

The Department shall maintain holding facilities that comply with applicable laws and regulations, in order to provide a safe environment for members and detainees.

Definitions

Detainee: A person who has been arrested or is in the custody of the Department.

Holding Facility: A temporary confinement cell or lockup where detainees are generally held for less than seventy-two (72) hours.

Design of Holding Facilities

Department holding facilities shall comply with Department of Public Health regulations and shall, at a minimum, be equipped with:

- Adequate lighting and air circulation;
- Access to a toilet and drinking water;
- Access to a wash basin and a bed with sanitary/fire-retardant bedding for each detainee held in excess of eight (8) hours;
- A first-aid kit, automatic fire alarms, smoke detectors, and adequate fire suppression systems;
- Audio and electronic (Watchman) monitoring system; and
- Posted signage regarding detainees' rights; obtaining medical services; and emergency evacuation.

Department holding facilities shall comply with the *Prison Rape Elimination Act (PREA) of 2003* and shall have signage posted advising detainees how to report incidents of sexual abuse and/or harassment.

Sanitation

Holding facilities shall be kept clean and sanitary, and shall be inspected:

- Before use by a detainee;
- Upon release of a detainee, and/or
- As necessary to prevent the spread of communicable diseases, as outlined in GEN-05 *Communicable Diseases*.

Cells and Keys

Cells that are:

- Ready for use shall be kept open and unlocked; or
- Not ready for use shall be kept closed, locked, and their not ready for use status posted.

Keys for the cells, and duplicates, shall be kept readily available at the barracks desk area.

Fire Prevention

- No matches, lighters, or smoking materials are allowed in any Department holding facility;
- Fire/smoke detection and suppression systems shall have written approval of fire officials;
- In the event of fire the local Fire Department of jurisdiction shall be notified and initial suppression efforts may be undertaken by member(s);
- An emergency evacuation plan shall be written and posted;
- At least one (1), preferably two (2), emergency exits shall be marked with a sign; and
- Any detainee that is evacuated will be handcuffed and secured in a cruiser. If necessary, the detainee will be transported to another barracks or authorized holding facility.

Electronic Monitoring

In addition to audio monitoring devices required by law, each holding facility shall have:

- A means of communication with the Station Desk Officer, or a panic alarm; and
- A video monitoring system so that each cell can be observed from the barracks desk officer area.

Guidebook

Troop Commanders shall ensure that a guidebook is kept at the desk or in the holding area of each facility, to assist the Station Desk Officer.

The guidebook shall contain information on:

- Holding facility operations;
- Procedures for escapes, fires, or suicide attempts;
- Available alternative lock-up facilities for juvenile offenders;
- The names and contact information for persons or organizations who will respond in the event of an attempted or threatened suicide;
- The names and contact information for persons or organizations who will respond in the event of an incident of sexual assault and/or sexual harassment; and
- List of available community Mental Health Resources including contact information.

Training

Members at a location where there are holding facilities/temporary detention room(s) shall receive training appropriate and consistent with each member's role, assignment and responsibilities in the holding facility/temporary detention room(s) including, but not limited to:

- The use of holding facilities, temporary detention room(s) or area(s), with retraining to occur at least once every three years;
- Suicide detection, intervention, and prevention;
- PREA Standards;
- Department policies regarding holding facilities, temporary detention room(s);
- Equipment related to the processing and detention of detainees and specific barracks detention operations;
- Use of physical restraints; and
- Operation of fire suppression equipment.

Pursuant to MGL c.40, § 36C, upon promotion, members shall receive refresher training in suicide detection, intervention, and prevention.

Access & Security

Facility security shall include securing doors or other means that may provide a potential avenue of escape for a detainee during booking and the temporary detention of a suspect. This includes, but is not limited to, sally port doors, potential avenues of escape from booking rooms, temporary detention rooms or other temporary holding facilities.

Non-essential persons shall not have access to the cell area, unless:

- Visiting a detainee, as outlined in DET-06 Detainee Monitoring**;** or
- No detainees are present, and the person(s) is accompanied at all times by a member.

Maintenance, sanitation, repair, or other outside personnel may have access to cells as necessary. Upon completion of the work, the cell area shall be inspected for tools or other items that may have been left behind.

Inspections

An inspection of each cell for weapons and contraband shall be made immediately prior to use.

Station Commanders are responsible for ensuring:

Frequency	**Item of Inspection**
Daily	• Fire detection and suppression equipment (visual inspection); • Cell bars, doors, locks, windows, ventilation, lights, monitors, and security devices; • First-aid kits, which will be replenished as necessary; • Tampering or damage to facilities; • Search for weapons or contraband; and • Sanitation, including vermin and pest inspection.

Inspections, continued

Frequency	Item of Inspection
Weekly	• Inspect the cell electronic monitoring device (Watchman) to ensure it is properly functioning; • Run a printout of the previous week's cell checks; • Examine the printout for compliance and discrepancies; and • Retain the weekly printouts for one (1) year.
Monthly	• Automatic Fire Alarm system test.
Semi-Annually	• Fire suppression equipment test; and • The review of the guidebook for accuracy.
Annually	• Administrative review of holding facilities and procedures to be completed concurrent with the Department of Public Health inspection.

Inspection records shall be maintained at the barracks for line and staff inspections.

Station Commanders shall ensure cooperation with state and local health and fire inspectors, pursuant to inspection requirements specified in 780 CMR The Massachusetts State Building Code (Appendix A).

To prevent inadvertent use, individual cells that do not pass inspection shall be kept closed, locked, and posted with an explanation of the deficiency.

Incidents

Detainees who cause damage to the cells may be subject to prosecution under MGL c.266, § 96, Defacement or Injury to a State Building.

Station Commanders shall make written reports to their Troop Commander of all incidents or conditions that threaten the holding facility or any person therein including detainees, or the ability of the barracks to safely hold detainees.

Troop Commanders shall immediately notify through channels, the Division Commander of Administrative Services, of all such incidents or conditions. The Division Commander of Administrative Services shall notify the Department of Public Health as required.

Subject: Holding Facility Design and Inspection	Number: DET-04

Temporary Holding Areas

Troop Commanders may authorize such temporary holding areas for the purpose of booking and bailing detainees, which shall provide for:

- Constant supervision of all detainees held in temporary holding areas;
- Immovable objects that are specifically designated for the purpose of booking and bailing detainees;
- Access to water and restrooms;
- Separation of male, female and juvenile detainees who are at high risk of being sexually assaulted;
- Fire prevention, evacuation, and suppression procedures; and
- Adherence to any applicable security procedures as outlined in Policy and Procedure.

Temporary Detention/Processing Room Administrative Review

- Barracks that do not have a holding facility shall ensure that rooms utilized for temporary detention receive regularly scheduled inspections for cleanliness and to determine if any unsafe conditions are developing. Deficiencies shall be addressed upon identification through the Station/Troop Commander; and
- Annually, Troop Commanders shall provide the Division Commander of Field Services an administrative report detailing adherence to Department policies and procedures governing temporary detention areas and whether alternative facilities are available for temporary detention.
  - This report shall be forwarded annually to the Division Commander of Field Services no later than November 30th.

References: DET-06 Detainee Monitoring;
DET-07 Detainee Sexual Assault and Harassment;
GEN-05 Communicable Diseases;
105 CMR 470;
780 CMR The Massachusetts State Building Code;
MGL c.40, § 36B;
MGL c.40, § 36C;
MGL c.111, § 21 and § 22;
MGL c.266, § 96;
Prison Rape Elimination Act (PREA) 28 CFR 115;
MPAC: 1.2.3, 33.8.2, 41.2.7, 71.2.1, 71.4.1, 71.4.2, 71.4.3, 72.1.1, 72.3.1, 72.3.2, 72.4.3,72.4.4, 72.4.5, 72.4.6, 72.4.7, 72.4.11, 72.6.2, 72.6.4.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**DET-05**

Subject:

Identification of Persons in Department Custody

Policy

All persons in Department custody must be properly identified prior to release. Fingerprints offer the most reliable means of individual identification. The submission and retention of fingerprint records and other biometrics create a reliable criminal history record. **Therefore, all persons arrested shall be fingerprinted and photographed**. In addition, all persons charged with a felony shall have their palmprints recorded if recording equipment is available. Persons taken into department custody for non-criminal reasons may be fingerprinted and photographed or may be identified through other means.

Definitions

AFIS (Automated Fingerprint Identification System): The computerized biometric matching system that stores identifying biometric templates and related demographics. The State AFIS maintains the following biometric information: known fingerprints and palmprints, latent fingerprints and palmprints, booking and tattoo photos, and iris images. AFIS is operated by the State Identification Section.

AFISR: An application available from the Department of Criminal Justice Information Services via single sign-on (DCJIS SSO). This application allows the review of Massachusetts fingerprint supported arrest records and the search of recent arrest submissions. This system can be searched by OBTN, Name, SID, and FBI number.

Biometrics: Distinctive, measurable physiological characteristics used to identify individuals. Commonly collected biometrics include fingerprints, palmprints, photographs (mug shots), and iris images.

Live Scan: Electronic fingerprint capturing devices that submit fingerprints, palmprints, and associated demographics and photographs to the State AFIS and NGI.

NGI (Next Generation Identification): A biometric matching system operated by the FBI that replaces the IAFIS system creating a national electronic repository of biometric and criminal history information.
www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi

Definitions, continued

OBTN/ SBTN (Occasion/Offense Based Tracking Number): A unique number assigned by the records management system associated with a specific event. This number allows the tracking of the individual event from arrest or summons through the state criminal history systems including AFIS and the courts.

SID (State Identification Number): A unique personal identifier based on a fingerprint ID and assigned by AFIS and the Identification Section.

UCN (Universal Control Number, formerly FBI number): Unique personal identifier based on a fingerprint ID and assigned by the FBI. This number is assigned to both criminal AND civil identities on file with the FBI.

Procedure for Properly Identifying Subjects

All persons arrested shall be fingerprinted and photographed. All persons charged with a felony shall have their palmprints recorded if recording equipment is available. Persons taken into department custody for non-criminal reasons may be fingerprinted and photographed or may be identified through other means.

Fingerprints and palmprints shall be captured and submitted to AFIS using the Live Scan device according to the *SIS-DOC 12-LIVESCAN Operational Guide*, which is located on Docushare.

The detainee's booking photo/mugshot shall be captured in RAMS.

Fingerprinting shall include the recording or annotation of all fingers and may include the recording of palmprints.

The following demographic information shall be included with all fingerprint submissions:

- OBTN/SBTN;
- Name;
- Date of birth;
- Sex;
- Race;
- Place of birth;
- Height;
- Weight;
- Eye color;
- Hair Color;
- Literal description of charges (not the chapter/section only);
- Date printed;
- Fingerprint official; and
- Date of arrest.

Procedure for Properly Identifying Subjects, continued

All Live Scan operators must properly log on and log off the system to prevent unauthorized access to the system. The operator logged on to the system will be documented as the fingerprint official on the official record.

Arrested persons shall not be considered eligible for bail until their fingerprints have been accepted and verified by AFIS. Fingerprint submission search results may be reviewed from the Live Scan or by viewing results in the DCJIS AFISR application. The *SIS-ADM-10 AFISR Procedural Guide* is available on Docushare.

Special Circumstances

In instances where Live Scan is not operational or available, the detainee may be:

- Transported for processing to a barracks where Live Scan equipment is available.

When the Live Scan and/or AFIS is not available and it is impractical to transport to another location, the detainee shall be:

- Processed using the traditional fingerprint card and inkpad method. The fingerprint card shall be sent immediately to the Identification Section via Troop mail for manual entry into AFIS.

- In circumstances where inked fingerprints are taken, a detainee may be considered eligible for bail consideration.

In instances when a subject's identity cannot be documented or when mutilated fingerprints are observed, the booking officer or desk officer may contact the Identification Section for review of the fingerprint record. The booking officer shall provide the SBTN/ OBTN.

Additionally, in situations when mutilated prints are observed, the Troop Duty Officer may contact the Crime Scene Services Section (CSSS) to assist in capturing full major case prints and/or ten-prints to assist in detainee identification.

Supervisors at the sub-station level and Cases and Reports Officer at the Troop level shall ensure:

- All officers are properly trained on the use of electronic fingerprinting/biometric capture equipment;
- All biometric processing equipment is operational;
- Proper supplies are available; and

Special Circumstances, continued

- Biometrics are properly captured and submitted to the Identification Section.

Identification Section
59 Horse Pond Road
Sudbury, MA 01776
24-hour contact 508-358-3170

Troop Commanders shall ensure overall compliance with this General Order.

References: SIS-DOC 12 LiveScan Operational Guide;
SIS-ADM 10 AFISR Procedural Guide;
SIS- ADM XX Mutilated Altered Print Recognition Guide;
MPAC: 1.2.5, 70.5.1, 82.1.2.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**DET-06**
Subject:	
Detainee Monitoring	

Policy

The safety and well-being of members and detainees is the Department's paramount concern and shall guide the application of this policy. Continuous supervision is essential for maintaining and ensuring the safety and welfare of both detainees in custody and the members responsible for monitoring them. To ensure the safety of all, necessary precautions shall be taken whenever a person is taken into custody.

Whenever a detainee enters a Massachusetts State Police (MSP) facility, the Desk Officer shall make an entry into the Daily Administrative Journal (DAJ) noting the date and time the detainee entered, the reason for detention, the condition of the detainee, any observed injuries, illness or complaints of pain. The Desk Officer shall log the date and time when a detainee leaves the facility. Only those room(s) and area(s) within the facility designed for detainee processing, testing, and temporary detention should be used for such purposes.

Conduct

Members shall not engage in speech or behavior that could be construed as inappropriate.

Detainee Rights

Detainees held in custody at any MSP facility shall be afforded all Constitutional rights and shall have, at a minimum, the following afforded:

- Timely court appearance;
- Opportunity to make bail;
- Confidential access to attorney(s) in a secure area free from monitoring within the facility;
- Access to a telephone; and
- Notification of the monitoring or recording of telephone conversations.

Detainees held over four (4) hours shall have meals provided at regular meal times, three (3) meals a day.

Detainees held over eight (8) hours shall be given access to a wash basin.

Detainee Rights, continued

Members receiving a call from a detainee's attorney are required to immediately inform the detainee of the attorney's attempt to reach them and to immediately relay the attorney's message to them, including, when applicable, a message advising them not to talk to investigators. An entry into the DAJ shall record the name of the member receiving the call, the name of the calling counsel including their Board of Bar Overseers (BBO) number and the name of the member delivering the message. (*Commonwealth v. McNulty* 458 Mass. 305).

Booking Process

Temporary detention rooms may include booking rooms and other area(s) specifically designated and/or designed for such purpose. Members utilizing said rooms shall have their portable radio on, or other means of direct communication with the Desk Officer available such as a panic/duress alarm.

Care should be taken to ensure that the temporary detention room/booking area is secured and free of items or hazardous materials that may be utilized to aid the escape of a detainee.

Firearms and Electronic Control Weapons (ECWs) **shall not** be carried on a member's person during the booking process, including, but not limited to, booking, fingerprinting, and the administration of the breath test.

Prior to initiating the booking process, the detainee shall be searched for weapons and contraband.

Arresting members are responsible for booking detainees. This shall include, when applicable, completing a booking sheet, conducting an inventory of the detainee's property, conducting any searches, fingerprinting, photographing, and administration of testing and secure detention. Additional members may be utilized to assist in the process and their assistance shall be detailed and logged into the DAJ.

The booking officer shall inform the detainee of his/her rights pursuant to Miranda by reading the Miranda Warning from a printed card or form.

The detainee shall be advised of his/her right to use the telephone and shall be afforded the use of a telephone within one hour of being brought in custody into a Department facility. The detainee may use the telephone to contact family or friends, to arrange for bail, or to contact an attorney. Members shall allow calls of a type, number and duration that are reasonable and practical, including contacting an attorney.

Booking Process, continued

The detainee may be allowed to use a personal cell phone or a Department phone. Toll calls will be made at the detainee's expense. If a detainee is provided a monitored or recorded telephone, they shall be informed of the monitoring (unless exempted by court order). If the detainee's primary language is not English, arrangements to convey this information via translator or language line shall be made.

The booking officer shall fingerprint and photograph all detainees under arrest and follow additional identification guidelines set forth in DET-05 Identification of Persons in Department Custody.

A detainee who actively resists arrest/booking and/or poses a threat to themselves or members should be placed in a cell until such time as the detainee becomes cooperative. A DAJ entry shall be made detailing the cause of delay in the booking process.

The booking officer shall conduct all detainee screening pursuant to the Prison Rape Elimination Act (PREA), suicide risk, medical conditions and advise detainees of all pertinent Constitutional rights.

In accordance with DET-07 Detainee Sexual Abuse and Sexual Harassment, when booking detainees, members shall screen all detainees to assess their risk of being sexually abused by other detainees or sexually abusive toward other detainees. Members shall also advise detainees of the Department's zero tolerance policy toward all forms of sexual abuse and sexual harassment towards any detainee. The screening and the advisement of the Department's zero-tolerance policy shall both be documented in RAMS/Department Records Management System.

An inventory search of the detainee shall be conducted at the time of booking consistent with DET-02 Custodial Inventory.

Detainees shall be handcuffed to the cuffing bar or other immovable object, which is specifically designated for that purpose.

Handcuffs may be removed to facilitate the administration of booking related duties including inventory, fingerprinting, photographing, and the administration of arrest related testing.

When more than one detainee is being booked at the same time, members involved in the booking process may consider use of the holding cell to limit interaction between detainees.

When arrested on a warrant, the detainee shall, upon request, be provided a printed copy of the warrant contained in the warrant management system within six (6) hours of the request.

Detainees under the influence of alcohol or drugs shall be afforded all administrative testing rights including but not limited to applicable rights

Booking Process, continued

pursuant to M.G.L. c. 263, § 5A. Members shall ensure such detainees are properly segregated from other detainees if warranted.

At no time should a member leave a detainee unattended outside the confines of the cell. Whenever a detainee is held in any temporary detention area outside the confines of the cell, the detainee should be under the continual, direct, physical supervision of a sworn member who can immediately intervene. Exception(s) may be warranted for detainee visitation with counsel and/or an interested adult.

Upon the conclusion of the booking procedures, the detainee should be placed in the appropriate cell.

- Prior to the placement of a detainee into a cell, a security check confirming the absence of weapons and/or contraband shall be made by the member placing the detainee into the cell.

The Desk Officer shall be advised of the cell placement, activate the audio/video monitoring and record the information in the DAJ. Cellblock assignment(s) shall adhere to the following:

- Female detainees shall maintain sight and sound separation from male detainees;
- Secure detention of juveniles shall adhere to the mandates of DET-09 Juvenile Detention; and
- Members shall adhere to the mandates of DET-08 Gender Identity and Expression.

Monitoring

The audio and video monitoring systems shall be used to continuously monitor the detainee's condition and shall be used as a means of two-way communication with detainees and other members in the cell block.

The audio and/or video monitoring systems shall not be used to unnecessarily violate the personal privacy of the detainee(s).

The Department shall provide 24-hour monitoring of detainees. The Desk Officer shall conduct a physical face-to-face check of all detainees every thirty (30) minutes, use the electronic monitoring (Watchman) device during the check and be responsible for logging the detainee check into the DAJ. Members making these checks shall have in their possession the keys to the cells in the event an immediate entry is required. Cell keys shall remain in the desk area, under control of the Desk Officer, outside of these checks.

Non-essential personnel are prohibited from all temporary detention areas and/or cellblocks whenever a detainee is present within said area(s).

Under no circumstances, shall non-essential personnel enter the cellblock area or other temporary detention area while detainees are in custody.

Monitoring, continued

The Desk Officer shall provide heightened protection to vulnerable detainees to include direct sight and sound supervision. The Desk Officer shall monitor the conduct and treatment of detainees or employees who reported sexual abuse and of detainees who were reported to have suffered sexual abuse pursuant to DET-07 Detainee Sexual Abuse and Sexual Harassment and DET-07A Detainee Sexual Abuse and Sexual Harassment Investigations, Review and Data Collection.

Meals may be provided from a correctional facility, detainee meal fund, the detainee's personal funds with their consent, or other appropriate source.

- The Desk Officer shall document within the DAJ the number, cost (if applicable), and type of meals served;
- Dishes, cups, and all utensils shall be used only once and secured upon completion of use; and
- Common cups and towels are not allowed.

Shift Change

The on-duty Desk Officer shall inform the incoming Desk Officer about the count and condition of the detainees. Incoming Desk Officers shall conduct a physical face-to-face check of all detainees to verify the count and condition of detainees prior to assuming desk duty. The incoming Desk Officer shall record this information into the DAJ.

Suicide Threats or Attempts

Information received from any source pertaining to a detainee's risk of harming themselves shall be considered valid.

If any of the following apply to the detainee:	Then:
• Makes a suicide threat or attempt; • Clearly exhibits signs or symptoms of suicidal behavior; • Has an entry in the Q-5 Query from a prior suicide threat or attempt at a detention facility; and/or • Has an entry in the Q-5 Query that did not occur at a detention facility.	• The Desk Officer shall assign a member to Q-5 watch; • The assigned member shall physically watch the detainee at all times; • The Desk Officer shall advise the Troop Duty Officer of the Q-5 watch; • The Desk Officer shall log the information related to the Q-5 watch in the DAJ; • The Desk Officer shall adhere to all other duties as outlined in the monitoring section of this policy; and • The detainee may be transported to a medical facility for evaluation;

Suicide Threats or Attempts, continued

If the detainee:	Then:
• Is not actively suicidal, but expresses suicidal ideation (e.g., expressing a wish to die without a specific threat or plan); and/or • Has a recent history of self-destructive behavior.	• The Desk Officer shall physically check the detainee on an unpredictable schedule at staggered intervals not to exceed every fifteen (15) minutes; • The Desk Officer shall record these checks utilizing the electronic monitoring (Watchman) device; and • The Desk Officer shall log these detainee checks into the DAJ.

If a detainee attempts or threatens suicide at an MSP facility, the following additional responsibilities apply.

Position	Duties

Desk Officer	• Contact EMS as necessary;
	• Provide medical attention as necessary;
	• Notify the Troop Duty Officer and Station Commander;
	• Document the incident in the DAJ; and
	• Pursuant to Massachusetts General Laws (MGL) c. 40, § 36A:
	  ○ Ensure the incident has been entered into the CJIS Q-5 suicide menu prior to the end of the shift; and
	  ○ Notify in writing any lockup facility the detainee is transferred to the exact nature of said attempt or threat.

Troop Duty Officer	• If needed, dispatch a supervisor to the barracks to assist; • Ensure the Desk Officer has assigned a member to Q-5 watch of the detainee; • Log the incident information into the DAJ; and • Ensure the provisions of M.G.L. c. 40, § 36A are followed.

Medical Care

Detainee Medications

Administration of medication shall be limited to prescribed medication in the detainee's name. Over the counter medication(s) shall not be administered to detainees.

Prescribed medications in the detainee's name and possession shall be taken into custody, recorded on the SP-2 Detainee Property Inventory and stored with the detainee's property. If the detainee so requests, the Desk Officer may allow a proper dosage, as prescribed on the medicine label, to be given to the detainee. Dosages and their frequency of ingestion shall not exceed the limitations set forth on the medicine container. Each dose of medication issued shall be recorded in the DAJ to include the name of medication, time distributed, and the member distributing the medication. Incoming Desk Officers shall be advised of relevant prescribed medication information including prior dosage distribution.

If there is any question concerning the administration of medications, the Desk Officer may either confer by telephone with a qualified medical physician before administering the medication, or if necessary, the detainee may be transported to a medical facility for the administration of medication. Alternatively, members administering medications may consult with a local pharmacist to confirm that medication is being properly administered, and that pills are properly identified as marked.

Sick or Injured Detainees

The procedures for requesting emergency health care shall be posted in a conspicuous place in English and any other language(s) prevalent within the barracks area.

When a member observes or is informed by a detainee that they are experiencing a medical problem that requires immediate medical treatment, the member shall request an ambulance. If unsure as to whether or not a detainee requires immediate medical treatment, members shall request assistance from trained medical personnel.

Pending arrival of EMS, members should provide basic First Aid if it is an emergency or appears serious. When possible, an additional member should be present, or notified to return to the barracks, prior to the detainee being removed for the administration of first aid.

Sick or injured detainees should not be transported by the Department, unless two (2) or more members are available for the transport. It may be more prudent to await the arrival of an ambulance.

- Upon arrival of an ambulance, members shall defer medical care to the EMTs but retain custody and security of the detainee;

Medical Care, continued

- A member shall follow directly behind the ambulance transporting the detainee to the medical facility to ensure custody of the detainee is continuously maintained during transport. If a member is requested by EMS to ride inside the transporting ambulance due to concerns about safety or flight risk regarding that detainee, another member in a cruiser shall then follow directly behind that ambulance; and
- The Troop Duty Officer shall be informed of any such incidents.

The Desk Officer shall advise the Troop Duty Officer of any medical care provided to a detainee at a barracks and/or during the transportation to and from an outside medical facility. Further, the Desk Officer is responsible for recording all information in the DAJ related to any medical care provided to a detainee at a barracks or during the transportation, temporary detention, and return of a detainee from an outside medical facility.

In the event of a sexual assault upon a detainee while in State Police custody by another detainee, staff member, employee or contractor, members shall adhere to the requirements of DET-07 *Detainee Sexual Abuse and Sexual Harassment.*

Guarding Detainees Off-Site

Injured or ill detainees transported to a medical facility for treatment or medication shall be handcuffed whether they are transported in a police vehicle or ambulance, unless physical disabilities prevent handcuffing. The removal of handcuffs should only occur when necessary to facilitate medical treatment. Prior to any such removal, measures to prevent escape, physical attack of, or by, the detainee shall be put into place where possible (e.g., cuffing of other hand, cuffing to bed/gurney).

The member assigned to guard the detainee will remain with the detainee at all times, whenever possible, during treatment. If it is medically necessary for a member to leave a detainee's immediate presence (e.g., to allow an x-ray), the member shall first ensure that all avenues of escape are secured and that there are no items accessible to the detainee that might be used as weapons.

In order to maintain the safety of members and the public, no outside communications shall be allowed by the detainee with others while at the hospital. Exception(s) to this are limited to medical staff administering aid, legal counsel, and/or an interested adult for the detainee.

Medical Care, continued

When a detainee is admitted to the hospital or remains there for a prolonged period, the member guarding the detainee should request the hospital personnel to 'block' the detainee's name, which would prevent the switchboard operator from re-routing a call to the detainee from an outside caller or allow others to know the detainee's location.

Use of utensils for detainee meals while at a medical facility will be screened and limited to prevent potential self-harm or harming of medical staff and/or any member(s).

Prior to returning the detainee to the barracks' cell, the detainee shall be searched to ensure that no weapon or contraband was concealed by the detainee while receiving medical care.

Discharge paperwork from a treatment facility shall be placed with the detainee's property upon return to the Department facilities.

Outside Deliveries

Detainees may only receive funds, prescription medications, or clean clothing from outside person(s).

All items shall be:

- Inspected for contraband and placed with the detainee's property, or provided to the detainee as appropriate;
- Documented on the detainee's SP 2 Detainee Property Inventory; and
- Logged into the DAJ.

Entering Cellblock

Firearms and ECWs shall be secured before entering an occupied cellblock, except when all detainees are secured in the cells and the 30-minute check is being conducted.

Members entering the cellblock alone shall maintain a means of communication by:

- Verbal communication with another member;
- Portable radio that is powered on; and/or
- Panic alarm or other means.

Department members shall announce themselves prior to entering the cellblock containing a detainee of the opposite gender. Staff should not intentionally place themselves in a position where they can view the breasts, buttocks, or genitalia of a detainee of the opposite gender when entering a cell or monitoring a detainee utilizing the audio/video monitoring system(s).

Detainees will be allowed to perform bodily functions without members or employees of the opposite gender viewing their breasts, buttocks or genitalia, except in exigent circumstances or when such viewing is incidental to routine cell checks.

Entering an Occupied Cell

Members shall only open or enter an occupied cell when:

- At least one (1) other member is present; or
- Releasing a detainee from custody; or
- In the event of an emergency.

Release of Detainee

When a detainee is removed from a cell, the cell shall be searched for weapons or contraband. If any damage is found to have been caused by the detainee, they should be criminally charged. Any unusual conditions shall be reported to the Station Commander and recorded by the Desk Officer in the DAJ.

Positive identification of the detainee shall be made prior to release by verifying the detainee's booking sheet photo or other photographic identification.

All items of property shall be compared to the items listed on the inventory report and the detainee requested to sign the form indicating that they have received the property. A refusal to sign shall be noted in writing on the inventory report and recorded in the DAJ.

The Desk Officer shall be responsible for recording in the DAJ information related to the release of the detainee from custody, including, but not limited to, the return of property, the cell inspection and the name(s) of the member(s) conducting such actions.

The release of a juvenile from Department custody shall be recorded in the DAJ consistent with the requirements of DET-09 Juvenile Detention.

Counsel / Interested Adult Visitation

Visitation with a detainee shall be limited to legal counsel and/or in the case of juvenile detainees an interested adult.

The Desk Officer shall be responsible for recording all information related to the visit in the DAJ.

<u>Visitor Requirements</u>:

- Show positive identification;
- Name, address and relationship to the detainee shall be documented in the DAJ;
- Counsel information shall include their BBO number;
- Checked for outstanding warrants and active court orders prohibiting contact (restraining/harassment prevention orders);
- Submit to a physical search and electronic scan for weapons and/or contraband;
- Submit to an inspection of their belongings for weapons and/or contraband prior to and immediately following the visit;

Counsel / Interested Adult Visitation, continued

- No physical contact with detainee;
- Prohibited from providing the detainee with any outside items; and
- Have no contact with or violate the privacy of other detainees.

Visitation Restrictions:

- Visitation will only be authorized when the Desk Officer can assign an available member to facilitate the visit;
- Visitation time limits shall be reasonable and not unduly interfere with member duties or otherwise interfere with barracks operations; and
- Visitation may be terminated at any time by the Desk Officer or member assigned for extenuating circumstances or violation(s) of visitor requirements.

Visitation shall be conducted in the following manner:

- If the cellblock is unoccupied the visit should take place in the cellblock with the detainee remaining in the cell and the visitor outside the cell;
- If the cellblock is occupied by other detainees, or at the request of the detainee's counsel or interested adult, the visit may take place in the booking room, temporary detention area or other room(s) specifically designated/designed for interviews and interrogations;
- The detainee shall be handcuffed in accordance with booking procedures if the visit takes place outside of the detainee's cell;
- Counsel or an interested adult shall not be allowed into the booking room, temporary detention area or other room(s) specifically designated/designed for interviews and interrogations until the detainee is properly secured;
- When available, the Desk Officer shall ensure the video monitoring system is activated but will disable the audio monitoring system to ensure the privacy of the visitation area;
- Provisions of INV-05 Special Protections for Juveniles shall be adhered to relative to visitation;
- Visitation that occurs at a medical facility should adhere to the requirements and restrictions as set forth in this policy within practical limitations; and
- The detainee shall be searched for weapons/contraband upon conclusion of the visit, prior to returning them to their cell.

Arraignment

Court in Session: If the court is in session when the booking process and all required reports are complete, it is the responsibility of the Desk Officer to arrange detainee transportation to the court of jurisdiction without delay.

Court not in Session: If the court is not in session when the booking process and all required reports are completed, the detainee shall be placed into a cell until bail can be arranged, or if bail cannot be arranged, until the next session of the court.

Arraignment, continued

Detainees who are not released on bail within twenty-four (24) hours following an arrest on charges for which probable cause has not been determined by a judge or magistrate are entitled to a probable cause hearing (i.e., "Jenkins Hearing" *Jenkins v. Chief Justice of District Court* 416 Mass 221, 1993). The arresting member or Desk Officer shall report the facts, orally or in writing, to a neutral magistrate. The results of the hearing shall be recorded by the Desk Officer in the DAJ. In the event that the review cannot take place due to extenuating circumstances, the hearing shall take place as soon as possible and the reason for the delay documented in the DAJ.

Bail

Arrestees shall be informed of the right to bail and afforded the opportunity for bail.

It shall be the responsibility of the Desk Officer to ensure that a detainee's opportunity to make bail is not impeded.

The Desk Officer shall contact the bail clerk to determine the bail set by the bail clerk.

Arrested persons shall not be considered eligible for bail until their fingerprints have been accepted and verified by AFIS.

Requesting Bail:

Prior to contacting the bail clerk, the Desk Officer should have, at a minimum, the following information available:

- Identity of the person to be bailed. If the identity is in question, the bail clerk shall be so advised;
- Demographic information, excluding race, related to the detainee collected during booking;
- Offenses charged;
- Criminal history to include Board of Probation (BOP) record and Interstate Identification Index (III); and
- Current detainee funds and whether or not the detainee wishes to be bailed.

Detainee Funds:

- The detainee shall be advised of his/her bail status. If the detainee has funds and wishes to be bailed, the bail clerk shall be so advised;
- If the detainee does not have funds and wishes to be bailed, the detainee may utilize the phone to arrange delivery of funds for bail;
- Upon arrival of the bail funds at the barracks, the Desk Officer shall contact the bail clerk; and

Bail, continued

- Funds provided for a detainee's bail shall be recorded in the DAJ and placed with the detainee's property with the SP-2 updated by the Desk Officer. Alternatively, person(s) providing funds for bail may wait for the arrival of the bail clerk in lieu of providing the funds in advance of the arrival of the bail clerk.

Detainees under arrest that are also in protective custody may be returned to custody after being bailed until such time as they may be released.

Receiving Detainees from an Outside Agency

- Desk Officers shall be responsible for the following when accepting detainees from an outside agency:
  - Verify the authority and lawfulness of the detention including identification of the presenting officer. If the presenting officer is not in uniform, a valid identification card shall be recorded and the Desk Officer may contact the requesting agency to verify the presenting officer's authority;
  - Obtain detainee information from the requesting agency. The information shall include:
    1. Positive identification of the detainee;
    2. A copy of the detainee's booking sheet;
    3. An official police report if the detainee is eligible to be bailed; and
    4. A point of contact and telephone number where a sworn member of the requesting agency can be reached at any time during the day or night.
  - The detainee shall be screened for PREA-related issues, suicide risk and medical conditions;
    1. If hospitalization, suicide watch, or other special handling is necessary, the requesting agency will provide the necessary personnel to manage these situations. Exceptions to this must be authorized by the Troop Duty Officer.
  - An inventory of the detainee's property shall be completed pursuant to this General Order;
  - Detainees may be bailed from custody if bail is set by the bail clerk in the jurisdiction of the delivering agency. The delivering agency shall be notified in advance of the bailing of the detainee; and
  - Pertinent information shall be entered into the DAJ consistent with information input during an MSP arrest/detention. This information shall include the contact information for the requesting agency.

Group Arrests/ Overcapacity Procedures

- If, as the result of a group arrest, or at any other time, the Station Commander or Troop Duty Officer determines that the number of persons to be detained in the holding facility will exceed the number for which the facility was designed, they may authorize the overcrowding on a temporary basis. The Desk Officer shall immediately notify the Troop Duty Officer or Station Commander of such conditions;
- In the event of a group arrest, detainees arriving at the barracks will be placed in a holding cell, with multiple detainees in a single cell if necessary, or otherwise secured as directed by the Station Commander or Troop Duty Officer;
  - Prior to the placement of any detainee(s) into a cell or temporary detention area(s), they shall be searched for weapons/contraband, screened for PREA-related issues, suicide risk and medical conditions.
- Area(s) of temporary detention shall be searched for weapons/contraband prior to the placement of any detainees within same;
- All detainee rights applicable to singular detention shall remain in effect during times of excess capacity;
- Monitoring of detainees shall adhere to all procedures set forth for the monitoring of singular detainees;
- Juvenile detention shall adhere to restrictions set forth in DET-09 Juvenile Detention;
- The Desk Officer is responsible for the accurate recording of information within the DAJ related to the booking and detention of all detainees;
- Non-violent, low security risk detainees may be held as a group if from the same incident or by gender affiliation and age in separate locations as determined by the Station Commander or Troop Duty Officer; and
- The temporary exceeding of capacity of this/these area(s) is permitted under these circumstances until such time as the excess capacity situation can reasonably be relieved, typically through the transfer or release of persons being held:
  - In order to accomplish this type of release, the Station Commander or Desk Officer shall examine the list of detainees and attempt to expedite the bail or release of the less serious offenders;
  - If release of a sufficient number of detainees to relieve the excess capacity of the holding facility is not possible, the Troop Duty Officer may authorize the excess detainees to be transported to other holding facilities in the Troop; and
  - The Troop Duty Officer is authorized to assign additional personnel as necessary to satisfy the staffing requirements of the exceeding capacity situation.

Escape or Wrongful Release

If a detainee escapes or is inadvertently released, the following actions shall be taken:

Position	Duties
Desk Officer	• Immediately notify the Troop Duty Office and Station Commander; • Notify area patrols and local departments of the escape; and • Make the appropriate DAJ entries.
Troop Duty Officer	• Immediately request K-9, Air Wing and other tactical resources as deemed necessary; • Dispatch a supervisor to the scene to: o Assume control of the recapture operation; and o Investigate the circumstances of the escape or wrongful release; o Prepare a report with findings and recommendations; • Notify the Troop Commander; • Notify GHQ Communications; • Notify the appropriate State Police Detective Unit (SPDU) of jurisdiction; and • Make the appropriate DAJ entries.
Troop Commander	• Notify the Division Commander; and • Review reports and take actions to prevent reoccurrences.
Division Commander	• Review reports and take actions to prevent reoccurrences.

Detainee Death Protocols

If a detainee dies while in a Department facility, the following actions shall be taken:

Position	Duties
Desk Officer	• Immediately notify the Troop Duty Officer and the Station Commander.
Troop Duty Officer	• Immediately notify the Troop Commander; • Immediately notify the SPDU of jurisdiction; • Notify the Office of the Chief Medical Examiner (OCME), as requested by SPDU; • Ensure that the appropriate DAJ entries are made; and • Ensure that proper procedures and provisions under M.G.L. c. 40, § 36A are followed.
State Police Detective Unit	• Respond to the scene and take command of the investigation.

Detainee Death Protocols, continued

Position	Duties
Station Commander	• Submit, within four (4) days, a report of the incident to the Troop Commander, along with all other related reports.
Troop Commander	• Immediately notify the Division Commander; • Assign a Commissioned Officer to immediately assist the SPDU investigation and to conduct an Administrative Review of the incident; • Forward copies of the reports to the OCME within seven (7) days; and • Review and submit reports and recommendations to the Division Commander.
Reviewing Commissioned Officer	• Assist the SPDU; • Conduct an Administrative Review of the incident to ensure that members followed Department procedures during the incident; and • Submit within four (4) days, a report to the Troop Commander.
Division Commander of Field Services	• Review reports and take actions to prevent reoccurrences; • Submit reports to the Deputy Superintendent for review and action; and • Maintain a file on detainee deaths.

References:
ADM-14 Personnel Investigation;
DET-02 Custodial Inventory;
DET-05 Identification of Persons in Department Custody;
DET-07 Detainee Sexual Abuse and Sexual Harassment;
DET-08 Gender Identity and Expression;
DET-09 Juvenile Detention;
DET-07 Detainee Sexual Abuse and Sexual Harassment;
DET-07A Detainee Sexual Abuse and Sexual Harassment Investigations, Review and Data Collection;
INV-05 Special Protections for Juveniles;
UOF-06 Electronic Control Weapons;
SP 2 Detainee Property Inventory;
M.G.L c. 40, § 36A Report of Death/Suicide Records;
M.G.L. c. 40, § 36C;
M.G.L c. 111, § 8 Use Common Drinking Cup;
M.G.L. c. 263, § 5A;
Commonwealth v. McNulty, 458 Mass. 305 (2010);
Jenkins vs. Chief Justice of District Court, 416 Mass 221 (1993);
SPAM Collective Bargaining Agreement Article 27;
Criminal Justice Information System (CJIS);
MPAC: 1.2.3, 33.8.2, 70.3.2, 71.1.1, 71.2.1, 71.3.1, 71.3.2, 71.3.3, 72.1.1, 72.1.2, 72.2.1, 72.4.1, 72.4.2, 72.4.3, 72.4.5, 72.4.7, 72.4.8, 72.4.9, 72.4.10, 72.5.1, 72.5.2, 72.5.3, 72.5.4, 72.5.5, 72.5.6, 72.5.7, 72.6.1, 72.6.4, 72.6.5, 72.7.1, 72.8.1, 72.8.2, 72.8.3, 72.8.4, 72.8.5.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**DET-07**
Subject:	
Detainee Sexual Abuse and Sexual Harassment	

Policy

In accordance with the *Prison Rape Elimination Act (PREA) of 2003,* the Department shall:

- Establish a zero tolerance policy toward all forms of sexual abuse and sexual harassment towards any detainee;
- Ensure that all detainees have the right to be free from sexual abuse and sexual harassment; and
- Establish a zero tolerance policy toward all forms of retaliation against anyone who reports sexual abuse and sexual harassment or who cooperates in a sexual abuse investigation.

This policy shall be made available through the Department's website and upon request.

Definitions

Detainee: Any person detained in a lockup, regardless of adjudication status.

Employee: A sworn member or civilian who works directly for the Department.

Gender Non-Conforming: A person whose gender identity (i.e., internal sense of feeling male or female) is different from the person's assigned gender at birth.

Holding Cell: Any secure enclosure that is under the control of law enforcement and is primarily used for the temporary confinement of suspects who have recently been arrested.

Intersex Individual: A person born with components of both male and female biological sex characteristics (genitalia, chromosomes, hormones, and secondary sex characteristics), or genitalia that are not clearly male or female.

Lockup: A facility that contains holding cells, cell blocks, or other secure enclosures that are:

- Under the control of a law enforcement, court, or custodial officer; and

Definitions, continued

- Primarily used for the temporary confinement of individuals who have recently been arrested, detained, or are being transferred to or from a court, jail, prison, or other agency.

Prison Rape Elimination Act (PREA): Signed into law on September 4, 2003. The Prison Rape Elimination Act establishes a standard of zero tolerance for rape and sexual assault or sexual harassment in any prison, jail, police lockup, or juvenile facility.

PREA Coordinator: A management level employee who oversees, develops, and implements Department efforts to comply with the PREA standards.

Sexual Abuse: Any sexual contact or the intentional touching of the victim's or suspect's genital, anal or other intimate area for sexual arousal or gratification, or for the abuse of either party; in this directive, includes in-custody sex offenses, voyeurism, or rape or attempts; harassment, sexual harassment, neglect, discrimination and similar terms. This policy applies to sexual abuse and/or harassment of a detainee by another detainee and/or sexual abuse of a detainee by an employee, contractor, or volunteer.

Sexual harassment includes:

- Repeated and unwelcome sexual advances, requests for sexual favors, or verbal comments, gestures, or actions of a derogatory or offensive sexual nature by one inmate, detainee, or resident directed toward another; and
- Repeated verbal comments or gestures of a sexual nature to an inmate, detainee, or resident by an employee, contractor, or volunteer, including demeaning references to gender, sexually suggestive or derogatory comments about body or clothing, or obscene language or gestures.

Voyeurism: When any employee, contractor, or volunteer invades a detainee's privacy for reasons unrelated to official duties, such as peering at a detainee who is using a toilet in their cell to perform bodily functions; requiring the detainee to expose their buttocks, genitals, or breasts; or taking images of all or part of a detainee's naked body or of a detainee performing bodily functions.

Department Responsibilities

The Department shall ensure that:

- An administrative or criminal investigation is completed for all allegations of detainee sexual abuse and/or sexual harassment pursuant to DET-07A Detainee Sexual Abuse and Sexual Harassment Investigations, Review and Data Collection;
- Alleged detainee sexual abuse and/or sexual harassment incidents, including third-party and anonymous reports, are reported to designated investigators;
- Detainees are informed of at least one way to report sexual abuse and/or sexual harassment to a public or private entity or office that is not part of the Department, allowing the detainee to remain anonymous if so requested;
- Investigators have received special training in sexual abuse investigations pursuant to Code of Federal Regulations (CFR) 28 CFR § 115.34;
- Develop an internal protocol appropriate for juvenile detainees where applicable; and
- Take appropriate measures to prevent retaliation against individuals who report and/or cooperate with an investigation.

Screening for Risk of Victimization and Abusiveness

In accordance with training, when booking detainees, sworn members shall screen all detainees to assess their risk of being sexually abused by other detainees or sexually abusive toward other detainees. Sworn members shall also advise detainees of the Department's zero tolerance policy toward all forms of sexual abuse and sexual harassment towards any detainee. The screening and the advisement of the Department's zero-tolerance policy shall both be documented in RAMS/Department Records Management System.

If after screening, the sworn member determines that the detainee may be at risk, the detainee shall be housed alone in a holding cell for the duration of his/her detainment at a State Police facility. This includes post-screening transportation in a Department vehicle to/from court, jail, prison, or other agency.

Staffing Plans

Station Commanders for each barracks containing cells shall develop and document a staffing plan that provides for adequate levels of staffing, and, where applicable, video monitoring to protect detainees against abuse.

Station Commanders shall consider the following factors when determining adequate staffing plans:

- The physical layout of the lock-up;
- The composition of the detainee population;
- The prevalence of sexual abuse incidents; and
- Any other relevant factor(s).

Each time the staffing plan is not complied with, the Station Commander shall document and justify all deviations from the staffing plan and shall forward the document with justifications to the PREA Coordinator.

Disabled Detainees

Detainees with disabilities include detainees who are deaf, hard of hearing, blind or have low vision, and those who have intellectual, psychiatric, or speech disabilities.

Sworn members shall take appropriate steps to ensure that detainees with disabilities have an equal opportunity to benefit from all aspects of the Department's efforts to prevent, detect, and respond to sexual abuse and sexual harassment. Such steps shall include providing access to interpreters who can interpret effectively, accurately, and impartially when necessary to ensure effective communication with detainees who are deaf or hard of hearing. In addition, sworn members shall ensure that written materials are provided in formats and through methods that ensure effective communication with detainees with disabilities.

Detainees with Limited English Proficiency

Sworn members shall take reasonable steps to ensure that detainees with limited English proficiency have meaningful access to information regarding the Department's policies and efforts to prevent, detect, and respond to sexual abuse and sexual harassment including by providing interpreters who can interpret effectively, accurately, and impartially.

Detainee Interpreters

No sworn member shall use detainees as interpreters or readers or otherwise request assistance from another detainee except in limited circumstances where an extended delay in obtaining an effective interpreter could compromise the detainee's safety, the performance of first-responder duties, or the investigation of the detainee's sexual abuse/harassment allegations.

First Responder Responsibilities

The first law enforcement sworn member to respond to a report of a sexual assault or sexual harassment shall:

- Immediately separate the alleged victim and abuser;
- Take immediate action to protect the detainee from substantial risk of imminent sexual abuse;
- Keep the detainee either with the officer or in the cell and under surveillance until a supervisor can investigate and determine any further actions to take to protect the detainee;
- Follow uniform evidence protocol that maximizes the potential for obtaining usable physical evidence including preserving and protecting any crime scene until appropriate steps can be taken to collect any evidence;
- If the abuse occurred within a time period that still allows for the collection of physical evidence, request that the alleged victim not take any action(s) that could destroy physical evidence, including, as appropriate, washing, brushing teeth, changing clothes, urinating, defecating, smoking, drinking, or eating;
- Offer all victims access to forensic medical examinations performed by a Sexual Assault Forensic Examiner (SAFE), Sexual Assault Nurse Examiners (SANEs) or qualified medical practitioner without financial cost to the victim, if evidentiary or medically appropriate;
- If the detainee is transported for a forensic examination to an outside hospital that offers victim advocacy services, ensure that the detainee be permitted to use such services to the extent available, consistent with security needs;
- Document all efforts to provide a SAFE or medical practitioner;
- Attempt to make a victim advocate from a rape crisis center or other facility available to the detainee if transported to a hospital or other medical facility consistent with security needs; and
- Accompany the victim through the forensic medical examination process and interviews.

First Responder Responsibilities, continued

If the first responder is not a law enforcement member, that responder shall:

- Request that the alleged victim not take any actions that could destroy physical evidence; and
- Immediately notify a law enforcement member.

Note: See also Policy and Procedure DET-07A Detainee Sexual Abuse and Sexual Harassment Investigations, Review and Data Collection.

PREA Coordinated Response Plan

If a detainee reports that they were sexually harassed while in a Department facility, the following actions shall be taken:

Position	Duties
First Responder	• Immediately separate the alleged victim and abuser; • Preserve and protect any crime scene until appropriate steps can be taken to collect any evidence; • Request that the alleged victim not take any actions that could destroy physical evidence, including washing, brushing teeth, changing clothes, urinating, defecating, drinking, or eating; • Take immediate action pursuant to this General Order; and • Immediately contact the desk officer.

PREA Coordinated Response Plan, continued

Position	Duties
Desk Officer	• Take immediate actions as a first responder pursuant to this General Order; • Notify, if necessary, local EMS and a local medical facility for an assessment of alleged victim's acute medical needs and to make an assessment of necessary treatment; • Immediately notify the State Police Detective Unit (SPDU)/Specialized PREA investigator(s) of jurisdiction; • Explain to the alleged victim the need for a forensic medical exam and offer the victim the option of undergoing one without any financial costs; • Make best efforts to ensure that examinations are conducted by Sexual Assault Forensic Examiners (SAFEs) or Sexual Assault Nurse Examiners (SANEs), or ensure that a qualified medical practitioner performs forensic medical examinations; • Offer alleged victim services by providing the victim with list of local sexual abuse advocates and/or crisis centers found in the Department's PREA brochure in DocuShare/PREA; • Ensure that the appropriate Daily Administrative Journal (DAJ) entries are made; • Immediately notify the Troop Duty Officer and the Station Commander; and • If the victim is transferred from the lockup to a jail, prison, or medical facility, inform the receiving facility of the incident and the victim's potential need for medical or social services, unless the victim requests otherwise.

PREA Coordinated Response Plan, continued

Position	Duties
Troop Duty Officer	• Immediately notify the Troop Commander and PREA Coordinator; • Ensure proper compliance with this General Order and DET-07A Detainee Sexual Abuse and Sexual Harassment Investigations, Review and Data Collection; • Provide for any special needs the victim may have; and • In the event that the victim is transferred from the lockup to a jail, prison, or medical facility, ensure that the receiving facility is informed of the incident and the victim's potential need for medical or social services, unless the victim requests otherwise.
State Police PREA Specialized Investigator(s)	• Respond to the scene and take command of the investigation; • Take all actions pursuant to DET-07A Detainee Sexual Abuse and Sexual Harassment Investigations, Review and Data Collection; • Inform the victim of his or her rights under relevant policies, federal and state laws; • Safeguard the custody of evidence; • Explain to the alleged victim the need for a forensic medical exam and offer the victim the option of undergoing one at no cost; • Offer the presence of a victim advocate or other staff member during the exam; • Interview the victim and any witnesses; • Submit report(s) of investigation pursuant to DET-07A Detainee Sexual Abuse and Sexual Harassment Investigations, Review and Data Collection; and • Document all referrals of allegations of sexual abuse or sexual harassment for criminal investigation.

PREA Coordinated Response Plan, continued

Position	Duties
Station Commander	• Submit, within four (4) days, a report of the incident to the Troop Commander, along with all other related reports.
Troop Commander	• Immediately notify the Division Commander; • Assign the PREA Coordinator to immediately assist the SPDU investigation and to conduct an Administrative Review of the incident; • Forward copies of the reports to the PREA Coordinator within seven (7) of their completion; and • Review and submit reports and recommendations to the Division Commander.
Reviewing Commissioned Officer	• Assist the SPDU; • Conduct an Administrative Review of the incident; and • Prepare a report for the Troop Commander within four (4) days. Note: The Administrative Review is to ensure that sworn members followed Department procedures during the incident.
Field Services Division Commander	• Review reports and take actions to prevent reoccurrences; • Submit reports to the Colonel/Superintendent for review and action; and • Maintain a file for PREA incident review pursuant to DET-07A Detainee Sexual Abuse and Sexual Harassment Investigations, Review and Data Collection.

Reporting

All employees shall immediately report to their immediate supervisor:

- Any knowledge, suspicion, or information regarding an incident of detainee sexual abuse and/or sexual harassment that occurred within a Department lockup;
- Any retaliation against detainees or Department employees who reported such an incident; and
- Employee neglect or violation of responsibilities that may have contributed to an incident or retaliation.

All allegations of sexual abuse, including third party and anonymous reports, shall be reported to a designated sexual abuse investigator who shall investigate the allegation pursuant to DET-07A Detainee Sexual Abuse and Sexual Harassment Investigations, Review and Data Collection.

Employees shall not reveal any information related to a sexual assault to anyone other than to the extent necessary to make treatment and investigatory decisions.

All verbal reports of sexual abuse and/or sexual harassment shall be documented by the immediate supervisor who receives a report of sexual abuse or sexual harassment pursuant to this policy.

Department employees may privately report sexual abuse and/or sexual harassment by contacting the PREA Coordinator, filing a complaint with the Office of Professional Integrity and Accountability, or utilizing the PREA third party contact number posted on the Department's website and on the PREA informational brochure.

Methods of reporting shall include: in-person, phone, mail, email, fax or any means by which the employee feels comfortable in reporting to a supervisor and/or the PREA Coordinator. Employees are expected to report any knowledge or suspicion of abuse. The methods of reporting are expected to vary based on the situation and the individual involved. Should there be any question as to the most appropriate method, the PREA Coordinator or Supervisor should be contacted.

Abuse Reports from Outside Facilities/ Agencies

An employee who receives an allegation that a detainee was sexually abused and/or sexually harassed while confined at a non-Department facility, shall notify through channels:

- The Colonel/Superintendent; and
- The Department PREA Coordinator.

Colonel/Superintendent shall:

- Notify the head of the facility or appropriate office of the agency where the alleged abuse occurred;
- Make notification, as soon as possible, but no later than seventy-two (72) hours after receiving the allegation; and
- Document such notification.

Training

All employees who may have contact with lockup detainees shall receive training regarding:

- The Department's zero-tolerance policy and detainees' right to be free from sexual abuse and sexual harassment;
- How to fulfill their responsibilities regarding prevention, detection, reporting, and response to sexual abuse and sexual harassment;
- The right of detainees and employees to be free from retaliation for reporting sexual abuse and sexual harassment;
- The dynamics of sexual abuse and sexual harassment in confinement;
- The common reactions of sexual abuse and sexual harassment victims;
- How to detect and respond to signs of threatened and actual sexual abuse;
- How to avoid inappropriate relationships with detainees;
- How to communicate effectively and professionally with detainees, including lesbian, gay, bisexual, transgender, intersex, or gender nonconforming detainees; and
- Compliance with relevant laws related to mandatory reporting of sexual abuse.

All employees shall annually review the PREA Standards Bulletin posted to DocuShare.

The Department shall provide each employee with refresher training annually to ensure that all employees know the agency's current sexual abuse and sexual harassment policies and procedures.

Training, continued

In years in which an employee does not receive refresher training, the Department shall provide refresher information on current sexual abuse and sexual harassment policies.

Every employee who may have contact with detainees shall acknowledge either in written or electronic format that they understands the Department's PREA policies and protocols and the PREA training they have received.

The Department shall maintain documentation confirming that employees, volunteers and contractors understand the training they have received.

PREA Coordinator

The Colonel/Superintendent shall:

- Designate a Detective Captain within Division of Investigative Services as the PREA Coordinator; and
- Ensure the PREA Coordinator has the authority to develop, implement, and oversee the Department's effort to comply with the PREA standards in all Department lockups.

The PREA Coordinator shall:

- Annually submit a status report of PREA compliance standards, investigative training requirements and reported/investigated incidents to the Colonel/Superintendent;
- Detail any corrective action required to ensure compliance with the PREA standard;
- Keep a current list of members who receive special training in sexual abuse investigations pursuant to Code of Federal Regulations (CFR) 28 CFR § 115.34; and
- Take necessary action to ensure Department compliance with the PREA standards subject to the Colonel's approval.

Hiring and Promoting Practices

The Department shall not hire or promote anyone who may have contact with detainees and shall not enlist the services of any contractor who may have contact with detainees who:

- Has engaged in sexual abuse in a prison, jail, lockup, community confinement facility, juvenile facility, or other institution (as defined in 42 U.S.C. 1997);
- Has been convicted of engaging or attempting to engage in sexual activity in the community facilitated by force, overt or implied threats of force, or coercion, or if the victim did not consent or was unable to consent or refuse; or

Hiring and Promoting Practices, continued

Has been civilly or administratively adjudicated to have engaged in the activity described in the paragraphs above.

The Department shall consider any incidents of sexual abuse and/or harassment in determining whether to hire or promote an employee, or to retain the services of any contractor, who may have contact with detainees.

Before hiring new employees who may have contact with detainees, the Department shall:

- Perform a criminal background records check on all applicants; and
- Make its best efforts to contact all prior institutional employers for information on substantiated allegations of sexual abuse, or any resignation during a pending investigation of an allegation of sexual abuse.

The Department shall ask all applicants and employees who may have direct contact with detainees about previous misconduct described in this section, in:

- Written applications and/or interviews for hiring or promotion; and
- Interviews or written self-evaluations conducted as part of reviews of current employees.

All employees shall disclose any of the misconduct described in this section.

Material omissions regarding such misconduct, or the provision of materially false information, shall be grounds for termination.

Any employee determined to have engaged in sexual abuse or sexual harassment of detainees as defined by policy shall be subject to discipline. The presumptive sanction for having engaged in prohibited behavior under this policy is termination.

Contractors and Volunteers

The Department shall perform a criminal background records check before retaining the services of any contractor or volunteer who may have contact with detainees and document the same. *See Vendor Acknowledgment PREA form.*

In the event that a contractor or volunteer has engaged in sexual abuse or has been convicted or adjudicated of having engaged in sexual abuse, they shall have no access or contact with detainees in Department custody.

The Department shall ensure that all volunteers and contractors who enter Department facilities and who may have contact with detainees have been trained on their responsibilities under the Department's sexual abuse and sexual harassment prevention, detection, and response policies and procedures including the Department's zero-tolerance policy regarding prohibited behavior.

The level and type of training provided to volunteers and contractors shall be based on the services they provide and the level of contact they have with detainees, but all volunteers and contractors who have contact with detainees, shall be notified of the Department's zero-tolerance policy regarding sexual abuse and sexual harassment and how to report such incidents. All volunteers and contractors who enter the Barracks and who may have contact with detainees shall sign an acknowledgement that they understand the Department's zero-tolerance policy and reporting requirements.

The Department shall maintain documentation confirming that volunteers and contractors understand the Department's PREA policy and information received.

Retaliation

The Department shall ensure that all detainees and employees who report sexual abuse or sexual harassment or cooperate with sexual abuse or sexual harassment investigations are protected from retaliation by other detainees or employees, and shall designate which employees or departments are charged with monitoring retaliation.

An employee who has knowledge, suspicion, or information regarding an incident of retaliation against detainees or employees who reported such an incident and any employee neglect that may have contributed to such retaliation, shall immediately report such incident or retaliation to their immediate supervisor.

Retaliation, continued

Supervisors who receive reports of retaliation shall employ multiple protection measures, which may include:

- Cell changes or transfers for detainee victims or abusers;
- Removal of alleged employees or detainee abusers from contact with victims;
- Providing emotional support services for detainees or employees who fear retaliation for reporting sexual abuse or sexual harassment or for cooperating with investigations; and/or
- Closely monitoring detainees or employees who fear retaliation.

Each Barracks Station Commander shall monitor all employee(s) who report sexual abuse or harassment to ensure that the employee(s) are not subject to retaliatory actions by other employees and shall document same.

Upgrades to Facilities and Technologies

When designing or updating holding cells, the Department will consider the effect of the design upon the ability to protect detainees from sexual contact.

When installing or updating video monitoring systems, the Department will consider how the technology may enhance the ability to protect detainees from sexual contact.

References:

DET-07A Detainee Sexual Abuse or Sexual Harassment Investigations, Review and Data Collection;
TRN-01 Training Administration;
Prison Rape Elimination Act (PREA);
Code of Federal Regulations (CFR) 28 CFR§ 115;
U.S. Department of Justice's Office on Violence Against Women publication, *A National Protocol for Sexual Assault Medical Forensic Examinations, Adults/Adolescents;*
Department of State Police Bulletin on PREA Standards;
Vendor Acknowledgement PREA Form.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**DET-07A**

Subject:

Detainee Sexual Abuse and Sexual Harassment Investigations, Review, and Data Collection

Policy

As the investigative agency for alleged sexual crimes committed on adults and juveniles held in a confinement setting by either the Department of Correction or Department of Youth Services, the Department of State Police shall ensure full compliance with the standards found within federal laws and mandates regarding the *Prison Rape Elimination Act* (2003).

This policy shall be made available through the Department's website and upon request.

Response

The Department shall adhere to the following requirements in regards to detainee allegations of sexual abuse and/or sexual harassment:

- Investigate allegations of sexual abuse and/or sexual harassment from the Department of Correction or Department of Youth Services;
- Investigate allegations of sexual abuse and sexual harassment from within the Department of State Police;
- Investigate allegations of sexual abuse and sexual harassment alleged by a detainee while detained at another facility;
- Follow uniform evidence protocol that maximizes the potential for obtaining usable physical evidence;
- Development of an internal protocol appropriate for juveniles where applicable;
- Offer all victims access without financial cost to forensic medical examinations performed by a Sexual Assault Forensic Examiner or qualified medical practitioner;
- Attempt to make a victim advocate from a rape crisis center available to the detainee;
- Accompany the victim through the forensic medical examination process and interviews; and
- Take appropriate measures to prevent retaliation against individuals who report and/or cooperate with an investigation.

Subject:	Number:
Detainee Sexual Abuse and Sexual Harassment Investigations, Review, and Data Collection	**DET-07A**

Special Training

Department Investigators shall receive special training in detainee sexual abuse and sexual harassment investigations according to Code of Federal Regulations (CFR) 28 CFR § 115.34, which shall include:

- Techniques for interviewing sexually abused or sexually harassed victims;
- Proper use of Miranda and Garrity warnings;
- Sexual abuse evidence collection in confinement settings; and
- The criteria and evidence required to substantiate a case for administrative action or prosecution referral.

Investigations

Department investigators when conducting an investigation into allegations of detainee sexual assault and/or sexual harassment, shall:

- Gather and preserve direct and circumstantial evidence, including any available physical and DNA evidence and any available electronic monitoring data;
- Interview alleged victims, suspected perpetrators, and witnesses;
- Review prior complaints and reports of sexual abuse and/or sexual harassment involving the suspected perpetrator;
- Notify their Division Commander through channels of the possible outcome when the evidence appears to support criminal prosecution; and
- Make relevant information regarding the status of the investigation available to the Department and/or requesting agency so that the detainee may be kept apprised of the investigation.

When there is probable cause to believe that a detainee had sexual contact with another detainee in a holding cell, or any Department employee had sexual contact with a detainee in a holding cell, the Department will make a criminal referral to the District Attorney's Office of jurisdiction or to the Attorney General's Office.

A criminal investigation will not be terminated because the alleged perpetrator separates from employment with the Department.

If an outside agency investigates allegations of sexual contact, the Department will cooperate with the investigators and remain informed about the progress of the investigation.

Note: See also Policy and Procedure DET-07 Detainee Sexual Abuse and Sexual Harassment for internal allegations.

Status Reports

Department Investigators who have conducted an investigation of a detainee's allegations of sexual abuse and/or sexual harassment shall:

- Make available to the requesting agency relevant information regarding the status of an investigation;
- Document that the detainee will be informed of the investigation status by the requesting agency; and
- Retain all written reports pertaining to the administrative or criminal investigation of alleged sexual abuse or sexual harassment in accordance with the Commonwealth's retention schedule or for as long as the alleged abuser is incarcerated or employed by the agency, plus five years, whichever is longer.

Sexual Abuse Incident Reviews

The PREA Coordinator in consultation with the Incident Review Team, which shall include the Station Commander, PREA Coordinator, and other pertinent individuals, shall conduct a sexual abuse incident review at the conclusion of every investigation into allegation of sexual abuse/harassment of a detainee in Department custody. Such review shall ordinarily occur within 30 days of the conclusion of the investigation. Such review will be conducted even when the allegation has not been substantiated, unless the allegation has been determined to be unfounded.

The review shall:

- Include input from supervisors and investigators as necessary;
- Consider whether the allegation or investigation indicates a need to change policy or practice to better prevent, detect or respond to sexual contact/abuse/harassment;
- Consider whether the incident or allegation was motivated by bias or gang affiliation;
- Examine the area where the incident allegedly occurred to assess whether physical barriers in the area may enable abuse;
- Assess the adequacy of staffing levels in that area during different shifts; and
- Assess whether monitoring technology should be deployed or augmented to supplement supervision by members.

The PREA coordinator shall submit a written report to the Colonel/Superintendent with findings and any recommendations for improvement.

The Department shall implement any recommendations for improvement or document its reasons for not doing so.

Subject:	Number:
Detainee Sexual Abuse and Sexual Harassment Investigations, Review, and Data Collection	**DET-07A**

Data Collection and Review

The PREA coordinator shall annually collect accurate, uniform data for every allegation of sexual abuse/harassment from each Barracks.

The incident-based data collected shall include, at a minimum, the data necessary to answer all questions from the most recent version of the *Local Jail Jurisdiction Survey of Sexual Violence* or other instrument developed by the Department of Justice and designated lockups.

The Department shall annually review data collected and aggregated in order to assess and improve the effectiveness of its sexual abuse prevention, detection, response policies, and training, including: identifying problem areas; taking corrective action on an on-going basis; and preparing an annual report of its findings from its data review and any corrective actions for each lockup, as well as the agency as a whole.

The PREA coordinator's annual report shall include a comparison of the current year's data and corrective actions with those from prior years and provide an assessment of the agency's progress in addressing sexual abuse. Upon approval of the Colonel, said report shall be made publicly available upon request, subject to redaction if appropriate.

The Department shall securely retain all incident based and aggregate data collected in accordance with all applicable data security policies and procedures.

All data collected shall be retained at least 10 years after the date of initial collection, unless federal, state, or local law requires otherwise.

Upon request, the Department shall provide the Department of Justice data from the previous calendar.

References:
Prison Rape Elimination Act of 2003, 42 U.S.C. c. 147 § 15601 et seq. (PREA);
Code of Federal Regulations (CFR) 28 § 115;
Local Jail Jurisdiction Survey of Sexual Violence;
DET-07 Detainee Sexual Abuse and Sexual Harassment;
TRN-01 Training Administration;
Garrity v. New Jersey, 385 U.S. 493 (1967);
Miranda v. Arizona, 384 U.S. 436 (1966).

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**DET-08**
Subject:	
Gender Identity and Expression	

Policy

The Department strives to ensure that everyone it serves is treated with dignity, respect, and professionalism. Department employees shall not engage in conduct that denigrates or shows hostility toward an individual because of their gender identity or gender expression.

Definitions

Adopted/Chosen Name: Non-birth name that an individual may use in self-reference. This may or may not be the individual's legal name and may or may not differ from the name on the individual's personal documents (i.e. driver's license, passport, etc.). Department employees should be aware that the use of an adopted/chosen name does not automatically equate to an attempt to hide one's legal identity, nor does it indicate that the individual is misrepresenting themselves.

Employee: A sworn member or civilian who works directly for the Department.

Gender Expression: External manifestations of gender identity such as an individual's name, personal pronouns, clothing, haircut, voice, and/or body characteristics.

Gender Identity: Gender identity is determined by an individual's self-identification and is different from an individual's sexual orientation. A person's gender-related identity, appearance or behavior, whether or not that gender-related identity, appearance or behavior is different from that traditionally associated with the person's physiology or assigned sex at birth. Gender-related identity may be shown by providing evidence including, but not limited to, medical history, care or treatment of the gender-related identity, consistent and uniform assertion of the gender-related identity or any other evidence that the gender-related identity is sincerely held as part of a person's core identity; provided, however, that gender-related identity shall not be asserted for any improper purpose.

Gender Non-Conforming: A person whose gender identity (i.e., internal sense of feeling male or female) is different from the person's assigned gender at birth.

Gender Non-Conforming Female: An anatomically born male who identifies as female. A *Gender Non-Conforming* female should be referred to as a female (i.e. she, her), regardless of medical history or the gender listed on identification documents.

Subject: Gender Identity and Expression	Number: DET-08

Definitions, continued

Gender Non-Conforming Male: An anatomically born female who identifies as male. A *Gender Non-Conforming* male should be referred to as a male (i.e. he, him, his), regardless of medical history or the gender listed on identification documents.

Intersex Individual: A person born with components of both male and female biological sex characteristics (genitalia, chromosomes, hormones, and secondary sex characteristics), or genitalia that are not clearly male or female.

Addressing an Individual

An individual may ask to be addressed differently from what his/her official identification documentation states. Therefore, when addressing individuals, Department employees shall adhere to the following:

- When uncertain which pronouns are appropriate, use the person's chosen name or respectfully ask the individual for clarification e.g., "How would you prefer to be referred to?";
- Address the individual by the name the individual chooses, regardless of whether or not the individual has obtained legal recognition of the chosen name;
- Use the titles and pronouns appropriate for the chosen name and/or gender expression (e.g., he/him for an individual identifying as male, she/her for an individual identifying as female, they/them for an individual identifying as another gender identity or whose gender identity is unknown, or as requested); and
- In all situations, make every effort to comply with the individual's requests in a non-judgmental, professional manner.

Official Documentation and Reports

An employee may observe that an individual's gender identity differs from the gender indicated on the individual's identification documents.

Employees encountering an individual wishing to be addressed differently from what is listed on official documents shall:

- Use the name and gender found on the individual's official documents in Department reports, i.e. incident reports, citations, and forms;
- Also document the individual's adopted/chosen name within the Department's Records Management System; and
- Use pronouns and descriptors consistent with the individual's gender identity when writing reports.

Searches

Department sworn members shall adhere to Massachusetts General Laws (MGL), Department Policy & Procedures, Department Rules & Regulations and constitutional provisions when conducting searches upon any individual.

When Department sworn members encounter *gender non-conforming* individuals, the members shall:

- Not perform a search or frisk for the sole purpose of determining an individual's gender;

Searches, continued

- Ask the individual what their preference is regarding the gender of the officer(s) searching the individual;
- Whenever practicable have two (2) officers of the preferred gender perform the search; and
- Document within the incident report the circumstances for the search, including the individual's preference regarding the gender of the officer(s) performing the search.

When an immediate cursory search for weapons is necessary for safety, the search may be conducted in the field by an officer of either gender.

Custody

If a gender non-conforming individual is being detained in a Department cell or vehicle, no other detainee(s) shall be housed in the same cell or placed or transported in the same vehicle if there are reasonable grounds to believe that the detainee's safety and security would be at risk.

Members transporting a gender non-conforming detainee shall radio their Station/Unit Desk Officer and have a Daily Administrative Journal (DAJ) entry made of the:

- Location;
- Preliminary charges against the detainee;
- Intended destination;
- Beginning odometer mileage, and upon arrival, the ending mileage; and
- If necessary, request for back up.

Gender non-conforming individuals may be held in Department custody pending bail, transported to another facility, or transported for court appearance as follows:

- The gender non-conforming individual shall be placed into a cell. If there are reasonable grounds to believe that the detainee's safety and security would be at risk, no other detainees shall be placed in that cell until the gender non-conforming individual is released from custody; or
- If there are other detainees in the cell(s), and there are reasonable grounds to believe that the gender non-conforming detainee's safety and security would be at risk, the gender non-conforming detainee shall be transported to the nearest station and be placed in a cell.

References: ADM-18 Anti-Harassment/Sexual Harassment and Discrimination;
DET-07 Detainee Sexual Abuse and Sexual Harassment;
Rules and Regulations Article 1.3 *Code of Ethics;*
Rules and Regulations Article 5.0 *Rules of Conduct;*
M.G.L.: C. 4 § 7;
Executive Order 526 *Order Regarding Non-Discrimination, Diversity, Equal Opportunity, and Affirmative Action;*
MPAC: 1.2.9.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
December 6, 2021	**DET-09**
Subject:	
Juvenile Operations	

Policy

The Department shall ensure protection of Constitutional rights and compliance with Federal and Massachusetts laws and regulations regarding the detention of juveniles.

When appropriate, safe, and feasible in determining how to respond to juveniles, members should use de-escalation strategies in an attempt to problem solve and provide alternatives to arrest. Members should consider all approved diversion options and select the alternative which least restricts the juvenile's freedom and provides an alternative compatible with the best interests of the juvenile and the community. When interacting with juveniles, members should make every reasonable effort to prevent an incident from escalating.

Steps should be taken to determine if juveniles in custody of the Department are alleged to have been harmed or to be in danger of harm including, but not limited to 51A's – Neglect or Abuse, 111B's – Protective Custody, 94C – Narcotics Violations. Members shall adhere to mandated reporting requirements pursuant to SOC-07C.

When a juvenile is arrested or placed into custodial protection, the member and their supervisor shall immediately review the most current version of M.G.L. c. 119, § 39H and § 67 to ensure proper legal treatment.

Juveniles

Juvenile: A child who is less than (eighteen) 18 years of age.

Under Age 12	A juvenile who is less than twelve (12) years of age cannot be charged with a crime.
Age 12 to less than age 18	A summons is the *preferred* method for bringing all juveniles to court, unless there is reason to believe the juvenile will not appear upon issuing a summons.
Arrest Warrant	An arrest warrant will issue if the court has reason to believe the juvenile will not appear upon a summons, or if the juvenile has been summoned and did not appear, or if the juvenile violated the terms and conditions of probation.

Status Offender

Status Offender: A juvenile who engages in an unlawful activity, which, if they were an adult, would be classified as non-criminal. Examples of juvenile status offenders are:

- Child placed into protective custody;
- Youth curfew violations (where applicable); or
- A "Child requiring assistance" from six (6) to eighteen (18) years of age per M.G.L. c. 119, § 39H who:
  - Repeatedly runs away from home;
  - Repeatedly fails to obey the lawful and reasonable commands of the child's parent, guardian or legal custodian;
  - Repeatedly fails to obey the lawful and reasonable regulations of the child's school;
  - Is habitually truant; or
  - Is a sexually exploited child.

NOTE: The Runaway Assistance Program (RAP) is a program designed to assist Police Officers who are dealing with runaways during the hours that juvenile court is closed (evenings, weekends and holidays). RAP provides a safe place where police can bring a runaway child, age 17 and under. After consultation with probation, and if the Police Officer determines that a child cannot be safely delivered to a parent or other responsible adult (including DCF), the Police Officer (or dispatcher) may call Mass211 by dialing "2-1-1" from any phone, including cell phones and when prompted dials "1-1" to speak with a Runaway Assistance Program (RAP) Specialist who can assist the officer in identifying the address of the closest Emergency Service Program (ESP) and the subsequent steps for the member to safely place the child. All contacts and placements shall be properly recorded by the member and/or the Desk Officer in the DAJ.

Delinquent Child

Delinquent Child: A child between twelve (12) and eighteen (18) years of age who commits any offense against a law of the Commonwealth; **provided, however, that such offense shall not include:**

- A civil infraction;
- A violation of any municipal ordinance or town by-law; or
- A first offense of a misdemeanor for which the punishment is a fine, imprisonment in a jail or house of correction for not more than six (6) months or both such fine and imprisonment.

Non-Secure Detention

Any juvenile who is under the age of (eighteen) 18, a status offender, or a juvenile in protective custody under M.G.L. c. 111B, § 8, shall be held in accordance with the requirements specified for non-secure detention of status offenders. These requirements are:

- The area where the juvenile is held is in an unlocked, multipurpose section, such as a report writing room or office;
- The space is in no way designed for residential use;
- The juvenile is held long enough to complete identification, investigation, and processing and then shall be released to a parent, guardian, legal custodian, other responsible adult, or transferred to an alternative juvenile facility or court;
- The juvenile is under continuous visual supervision by a sworn member until released; and
- At no time is the juvenile to be handcuffed to any stationary object.

Note: A status offender may be handcuffed, but not to a stationary object, which shall not be considered "secure detention".

Juveniles under the age of fourteen (14), status offenders, or juveniles in protective custody shall not be placed in a cell.

Secure Detention

Secure detention is defined as physically detained or confined in a room, set of rooms, or a cell that has the ability to lock an individual within. Secure detention can result from either being placed in such a room and/or from being physically secured to a stationary object such as a cuffing rail/bench. Please note that at no time is a juvenile to be secured to a stationary object.

Alternative Enforcement Considerations

Members conducting enforcement of criminal and civil violations of Massachusetts law with juveniles should use the least coercive reasonable alternative where applicable. Options for enforcement may include the following and should be based upon the totality of circumstances present at the time of enforcement action:

- Release forthwith along with no further action; or
- Issuance of citation and/or summons in lieu of custody in accordance with Massachusetts law and Department policy; or
- Custody in accordance with Massachusetts law and Department policy.

Procedures for the Detention of Juveniles

Members shall adhere to the following when detaining juvenile(s):

- A juvenile may not be held in police custody for longer than six (6) hours;
- A juvenile in Department custody should only be held long enough for members to complete the identification and booking process. Once the identification and booking process is complete, the juvenile must be:
  - Transported to the juvenile court; or
  - Released to their parent/guardian/custodian; or
  - Transferred to the custody of the Overnight Arrest Program (after 1800hrs on weeknights and anytime on the weekends/holidays).
- A juvenile who is under the age of fourteen (14) shall not be placed in secure detention for any amount of time;
- No juvenile between fourteen (14) and eighteen (18) years of age shall be placed in a cell, unless the cell has been certified by the Department of Youth Services (DYS);
- A juvenile who is securely detained in Department custody must be separated by sight and sound from adults in custody;
- A juvenile, placed in Protective Custody for alcohol, **CANNOT BE SECURELY DETAINED** for any amount of time;
- A juvenile, placed in Protective Custody for controlled substances/toxic vapors, **MUST be transported to an appropriate emergency medical treatment facility;** and
- A juvenile, placed in custody in accordance with a Child Requiring Assistance (CRA) matter, **CANNOT be brought to the barracks.**

Juvenile Arrest Delinquent Offense

When a juvenile is placed under arrest, the Troop Duty Officer, or designee, shall immediately notify at least one (1) of the child's parents, or, if there is no parent, the guardian or custodian with whom the child resides or the Department of Children and Families (DCF).

If Arrest Occurs during Court Hours	Members must complete the booking process and then transport the juvenile to the Juvenile Court of jurisdiction.
If Arrest Occurs after Court Hours	The Troop Duty Officer, or designee, will make a determination whether to release or detain the juvenile based on the totality of the circumstance present, consistent with Department policy. There is no longer a statutory requirement for the police to contact a Juvenile Probation Officer, and as such, the Probation Department has ceased its on-call program.

Juvenile Arrest Delinquent Offense, continued

If Arrest Occurs after Court Hours	Release: If a juvenile has been arrested without a warrant and the Troop Duty Officer, or designee, determines that the juvenile should be released, such release shall be done upon the acceptance of the written promise from the parent, guardian, custodian, or a representative of DCF, who will ensure the juvenile's appearance in court. The Troop Duty Officer, or designee, will ensure that members utilize the SP 122 Written Promise form to obtain the required written promise. The released juvenile shall be advised that they must appear in the Juvenile Court of jurisdiction on the next business day. The Troop Duty Officer, or designee, shall ensure that the appropriate Juvenile Court and appearance date are noted on the SP 122 Written Promise Juvenile Form. Detain: If a juvenile between fourteen (14) and eighteen (18) years of age has been *arrested on a warrant* or if the Troop Duty Officer, or designee, *requests in writing that such a juvenile be detained*, the Troop Duty Officer, or designee, shall contact the Bail Magistrate/Bail Commissioner. In accordance with M.G.L. c. 119, § 67, a juvenile age twelve (12) or thirteen (13) *who has been arrested without a warrant* is prevented from being admitted to bail and therefore must be released to a parent, guardian, custodian, or a representative of DCF.
Bail	The Bail Magistrate / Bail Commissioner will set bail and/or terms and conditions of release based on the juvenile's current charge(s), circumstances of the arrest, criminal history and/or as directed by the arrest warrant.

Juveniles in police custody must be held sight and sound separate from adult detainees.

A juvenile charged with delinquency offenses *shall not be held* in a police lockup or otherwise securely detained for any *longer than six (6) hours*. If the juvenile is placed in a cell, the cell must be a DYS certified cell. All DYS certified cells shall be posted or marked.

The requirement not to release a defendant for six (6) hours when arrested for a violation of M.G.L. c. 209A or M.G.L. c. 265, § 13M (Domestic Assault or Domestic Assault and Battery) or § 15D (Strangulation or Suffocation), ***DOES NOT apply to juveniles***.

Juvenile Arrest Delinquent Offense, continued

A juvenile in Department custody should be held only long enough for members to complete the identification and booking process. Once the identification and booking process is complete, the juvenile must be either:

- Transported to the juvenile court, or
- Released to their parent/guardian/custodian/DCF representative, or
- Transferred to the custody of the Overnight Arrest Program (after 1800hrs on weeknights and anytime on the weekends/holidays).

The best practice is for the six (6) hour clock to start when the juvenile is placed in police custody and ends when custody is:

- Transferred to the juvenile court, or
- The juvenile is released to their parent/guardian/custodian/DCF representative, or

Custody is transferred to the Overnight Arrest Program.

Juvenile Unable to Make Bail / Unable to be Released

When a juvenile has been charged with a delinquency or youthful offender offense and is unable to make bail or is unable to be released and court is closed, the Troop Duty Officer, or designee, must contact the Department of Youth Services Central Referral Line at 617-474-8150 or 617-474-8179 to coordinate DYS placement (after 1800hrs on weeknights and anytime on weekends/holidays). The Troop Duty Officer, or designee, shall ensure that DYS is provided with information regarding the juvenile's arrest and is advised of the bail amount as it relates to the bail fee and bail.

If a juvenile is being held on a bail fee only ($40.00 - Personal Recognizance), DYS has no authority to hold the juvenile in its custody. The Troop Duty Officer, or designee, shall inform the bail magistrate / bail commissioner of this and arrangements will be made to release the juvenile without imposing a Bail Fee.

- If the juvenile is in the custody of DCF, DCF shall be notified via the DCF hotline, 800-792-5200, to take custody of the juvenile.
- If a parent, guardian or custodian refuses to take custody of a juvenile who is otherwise eligible to be released, the Troop Duty Officer, or designee, shall file a 51A and notify DCF via the DCF hotline for placement.

DYS will provide the Troop Duty Officer, or designee, with the location of the Overnight Arrest Program.

- If the juvenile is *suffering from any medical condition(s)*, including, but not limited to alcohol and/or drug impairment, suicidal tendencies, UOF requiring medical attention, they *must be medically cleared prior to placement*.
- The Troop Duty Officer, or designee, is responsible for obtaining any current medications for the juvenile.
- The Troop Duty Officer, or designee, must provide a copy of the Booking Sheet prior to placement.

Juvenile Unable to Make Bail / Unable to be Released, continued

It is the Department's responsibility to transport the juvenile to the Overnight Arrest Program.

It is also the Department's responsibility to transport the juvenile from the Overnight Arrest Program to the juvenile court of jurisdiction before 0900 hours.

Protective Custody of Juveniles Present Where Controlled Substances Are Unlawfully Kept or Possessed

M.G.L. c. 94c, § 36 requires: If a police officer finds a child present where said officer finds a substance which he reasonably believes to be a controlled substance listed in Class A, B, or C of section thirty-one kept or possessed in violation of any provision of this chapter, and if the police officer reasonably believes that the child has not reached his eighteenth birthday and that the child knew of the presence of such controlled substance, the police officer may lawfully take such child into protective custody for a period not to exceed four hours. Persons having custody of a child under this section shall make reasonable efforts to notify the child's parent or guardian or other person having lawful custody. Such persons shall be considered to be acting in the conduct of their official duties and shall not be held criminally or civilly liable for such acts. A child detained pursuant to the provisions of this section shall not be considered to have been arrested or to have a criminal record for any purpose; however, only a departmental record of custody shall be made by the officer indicating the circumstances of custody. The procedures and processes provided by this section for the care, protection, and custody of children are not exclusive but are in addition to all others provided by law.

Transportation of Juveniles

Juveniles may be:

- Transported in marked or unmarked vehicles.

Juveniles shall not be:

- Transported with adult detainees; or
- Transported to court or any other institution in patrol wagons pursuant to M.G.L. c. 119, § 34.

Jenkins Hearing

If a juvenile is arrested without a warrant and held in custody (to include while being held at the Overnight Arrest Program), for more than twenty-four (24) hours, they are entitled to a Jenkins *hearing* to determine whether or not there was probable cause to make the arrest and to continue to hold the juvenile.

- If the juvenile will be held for over twenty-four (24) hours, in order to facilitate a *Jenkins* determination of probable cause to continue to hold the juvenile, the Troop Duty Officer, or designee, must call a bail magistrate / bail commissioner.
- The bail magistrate / bail commissioner that set bail on the juvenile cannot be the same magistrate/commissioner who conducts the *Jenkins* hearing.

Special Considerations

Members may have to take extra steps to ensure that juveniles understand their rights. This may include explaining or repeating the *Miranda* rights, or explaining Department procedures or juvenile court procedures to the juvenile. Refer to INV-05 Special Protections for Juveniles for procedures regarding the interrogation of juveniles.

Barracks Juvenile Officers

Station Commanders shall:

- Designate a barracks court officer as the Juvenile Officer;
- Ensure that Juvenile Officers attend specialized training, if required;
- Ensure that M.G.L. c.119, § 39H and § 67 are followed.

Filing

Station/Section Commanders shall maintain a separate, secure file accessible only by authorized personnel, containing all of the identifying data of each juvenile arrest and any related reports.

Records involving criminal charges against juveniles shall be maintained separately from other records.

Access to electronic juvenile records shall require system access limited to authorized personnel utilizing password protection.

The retention and/or expungement of juvenile records shall be governed by the Massachusetts Public Records Law and/or a valid court order. The Department shall adhere to the Massachusetts Statewide Records Retention Schedule, including the disposition of juvenile records after attaining adult age. Expungement of barracks juvenile records shall be administered by the Station Commander pursuant to Department policy in accordance with the Massachusetts Statewide Records Retention Schedule. DAS shall administer the retention/expungement of juvenile records at the Department level.

Administrative Journal Records Reporting Juvenile Detentions

The Daily Administrative Journal (DAJ) shall:

- Contain all required information except the juvenile's name, address, date of birth (DOB), and any other identifying data; and
- Under the "name" section the word "JUVENILE" shall appear, followed by a sequential number starting with "#1" for the first juvenile arrested that year.

A separate record shall be maintained that links Juvenile Arrest Journal numbers and juvenile identifying information. This record shall not be released to the public and/or media.

Dissemination of juvenile records shall be authorized by the Station Commander, and/or a Supervisor, for a legitimate law enforcement purpose or by court order. The dissemination of a juvenile record shall be recorded in the DAJ identifying the agency record released, the entity to which the record was released, and ensuring a reference to only the JUVENILE#. The DAJ shall contain only the juvenile number and no other personal data.

Subject:	Number:
Juvenile Detention	**DET-09**

Reporting Juvenile Detention

Barracks that have cells approved for juvenile use are administratively required by the Executive Office of Public Safety & Security (EOPSS) to submit a monthly lockup docket, as directed within CJIS Extranet.

EOPSS may contact a barracks that has arrested a status or juvenile offender, to ensure compliance with the applicable holding laws. EOPSS utilizes the information to monitor the Commonwealth's compliance with state law and the Federal Juvenile Justice and Delinquency Prevention Act of 1974 and 2002. All members shall assist EOPSS as requested.

References

M.G.L. c. 94C, § 36;
M.G.L. c. 111B, § 8;
M.G.L. c. 119, § 34;
M.G.L. c. 119, § 39H;
M.G.L. c. 119, § 51A;
M.G.L. c. 119, § 54;
M.G.L. c. 119, § 52;
M.G.L c. 119, § 67;
Jenkins v. Chief Justice of the District Court, 416 Mass. 221 (1993);
Massachusetts Statewide Records Retention Schedule;
INV-05 Special Protections for Juveniles;
DET-03 Detainee Transportation;
SOC-07C Abuse of Children/Disabled/Elderly;
SP 122 Written Promise Juvenile Form;
MPAC: 1.2.3, 1.2.6, 1.2.7, 44.2.1, 44.2.2, 72.5.3, 82.1.2.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**DET-10**
Subject:	
Protective Custody	

Policy

The Massachusetts State Police shall comply with the requirements of Massachusetts General Law Chapter 111B and Massachusetts General Law Chapter 111E when taking an incapacitated person into protective custody.

Definitions

Assisting Officer: Sworn member placing a person into protective custody.

Facility: Any public or private place, or portion thereof, providing services especially designed for the detoxification of persons.

Incapacitated: The condition of a person who, by reason of the consumption of alcohol and/or a controlled substance, toxic vapor, or other substance other than alcohol, is:

- Unconscious; or
- In need of medical attention; or
- Likely to suffer or cause physical harm or damage property; or
- Disorderly.

To place a person into protective custody, an officer needs probable cause to believe that the person is incapacitated.

Intoxication alone is not sufficient to warrant a finding of incapacitation.

Juvenile: A child who has not yet attained their eighteenth (18) birthday.

Protective Custody

Pursuant to M.G.L. c.111B, § 8: Any person who is incapacitated due to consumption of alcohol may be assisted by a police officer with or without the person's consent to the person's residence, to a facility, or to a police station.

Subject:	Number:
Protective Custody	**DET-10**

Protective Custody, continued

Pursuant to M.G.L. c.111E, § 9A: Any person who is incapacitated due to consumption of substance(s) other than alcohol may be placed into protective custody by a police officer without the person's consent for the purpose of immediately transporting the person to an acute care hospital or satellite emergency facility or otherwise immediately obtaining appropriate emergency medical treatment.

Procedure for Taking Person into Protective Custody

	111B § 8 (Alcohol)	**111E § 9A (Substance other than Alcohol)**
Determination of Incapacitation is a Two-Step Process	**Step One: Assessment of Incapacitation** A person who, by reason of the consumption of alcohol, is: • Unconscious, or, • In need of medical attention, or • Likely to suffer or cause physical harm or damage property, or • Disorderly is deemed incapacitated. **Step Two: Assessment of Intoxication** *Right to a Breathalyzer Test* (BT) - Any person assisted by a police officer to a police station shall have the right, and be informed in writing of said right, to request and be administered a breathalyzer test. *Presumption of Intoxication* - Any person who has a BT of (.10) or above is presumed intoxicated. *Sobriety Testing* - If any person has a BT of .06, .07, .08 or .09, police are authorized to administer sobriety testing in order to determine whether to release or hold the person.	**Step One: Assessment of Incapacitation** A person who, by reason of the consumption of substance other than alcohol, is: • Unconscious, or, • In need of medical attention, or • Likely to suffer or cause physical harm or damage property, or • Disorderly is deemed incapacitated. **Step Two: Assessment of Intoxication** A police officer may ask a person to consent to reasonable tests of coordination, coherency of speech, and breath to determine if the person is incapacitated. A police officer may place the person into protective custody when such tests or other information or observations indicate that the person is incapacitated.

Procedure for Taking Person into Protective Custody , continued

	111B § 8 (Alcohol)	**111E § 9A (Substance other than Alcohol)**
	Release Forthwith – Unless there are pending charges or a warrant, any person who has a BT (.05) or less shall be released from custody forthwith. *However*, if a minor registers *any* BT reading, the minor must be released to a parent, guardian, or responsible adult.	
Role of Police Officer when taking a person into Protective Custody:	A police officer shall assist an incapacitated person by bringing him or her to: • That person's residence; or • A police station (will have to notify facility); or • A facility (as defined above). *NOTE:* If a person is brought to a police station, that person has the right to: • Request and be administered a breathalyzer test; and • Make a phone call.	A police officer shall assist an incapacitated person by: • Immediately transporting the person to an acute care hospital or satellite facility; or • Obtaining appropriate immediate emergency medical treatment (EMT) for the person.
Notification of Facility	If any incapacitated person is assisted to a police station, the officer in charge, or designee, shall notify forthwith the nearest facility that the person is being held in protective custody. If suitable treatment services are available at a facility, the department shall thereupon arrange for the transportation of the person to the facility. The officer in charge, or designee, shall ensure that a Daily Administrative Journal (DAJ) entry indicates: • The name of the facility notified; and • If transportation was arranged.	N/A

Procedure for Taking Person into Protective Custody , continued

	111B § 8 (Alcohol)	111E § 9A (Substance other than Alcohol)
Juveniles	The parent, guardian or legal custodian of any juvenile to be held in protective custody at a police station, shall be notified forthwith upon his/her arrival at said station or as soon as possible thereafter. Any juvenile who is held in protective custody at a police station shall, upon request of his or her parent, guardian or legal custodian, be released to the custody of said parent, guardian or legal custodian. A juvenile placed in protective custody, for alcohol, cannot be securely detained for any amount of time. Members shall ensure that detention of juveniles shall conform to General Order DET-09 Juvenile Detention.	The parent, guardian or legal custodian of any juvenile placed into protective custody shall be notified as soon as practicable. A juvenile placed in protective custody, for controlled substances/toxic vapors, must be transported to an appropriate emergency medical treatment facility.
Time Restraints	**No adult shall be held more than 12 hours** - No person assisted to a police station shall be held in protective custody against a person's will; provided, however, that if suitable treatment at a facility is not available, an incapacitated person may be held in protective custody at a police station until a person is no longer incapacitated or for a period of no longer than twelve hours, whichever is shorter.	A person cannot be held in protective custody beyond the time required to complete the transport of the individual to an acute care hospital or satellite emergency facility or to obtain immediate emergency medical treatment. Legislation does not provide a time frame for how long transport would take to be completed or medical treatment sought.
Use of Force	Reasonable force may be used to take a person into protective custody.	
Search and Inventory Items	Officers may search the person and immediate surroundings for weapons. Any items seized will be inventoried and returned if lawfully possessed.	

Procedure for Taking Person into Protective Custody , continued

	111B § 8 (Alcohol)	111E § 9A (Substance other than Alcohol)
Documentation	An entry of custody in the report narrative shall be made indicating: • The date, time, place of custody; • The name of the assisting officer; • The name of the officer in charge; • Whether the person held in custody **exercised his or her right to make a phone call**; • Whether the person held in custody **exercised his or her right to take a breathalyzer test**, **and** the **results of the breathalyzer test if taken**; and • The name of the facility notified and if transportation was arranged. An SP 850 Protective Custody form demonstrating subject was read and understood these rights must be completed.	An entry of custody in the report narrative shall be made indicating: • The date, time, place of custody; • The name of the assisting officer; • The name of the officer in charge; and • The name of the facility to which the person was transported.
Status of Protective Custody	Not an arrest	
Additional Considerations	If a member subsequently places into protective custody a subject who has been bailed after having been arrested for OUI-Alcohol, the member shall process the subject according to MGL c. 111B and this General Order. Refer also to TRF-14 Operating Under the Influence.	If a subject has been revived using naloxone ("Narcan") and has regained consciousness, it may still be appropriate to place the subject into protective custody and transport that subject for medical attention, if the training and experience of the officer indicate that further medical attention is appropriate.

Procedure for Taking Person into Protective Custody , continued

	111B § 8 (Alcohol)	111E § 9A (Substance other than Alcohol)
Additional Considerations	If a member subsequently places into protective custody a subject who has been bailed after having been arrested for OUI-Alcohol, the member shall process the subject according to MGL c. 111B and this General Order. Refer also to TRF-14 Operating Under the Influence.	If a subject has been revived using naloxone ("Narcan") and has regained consciousness, it may still be appropriate to place the subject into protective custody and transport that subject for medical attention, if the training and experience of the officer indicate that further medical attention is appropriate.

Protective Custody of Children in the Presence of Controlled Substances

According to M.G.L. c. 94C § 36, members may place a child into Protective Custody for no more than (4) four hours if:

- The member(s) reasonable believe the child has not reached their (18^{th}) eighteenth birthday; and
- The child in the presence of a Class A, B, or C of c. 94c § 31; and
- The member(s) reasonable believe the controlled substance is in violation of c. 94C § 31; and
- The child knew of the presence of the controlled substance.

Persons having custody of the child shall make reasonable efforts to notify the child's parent, guardian, or person having lawful custody. The person shall be considered acting in the conduct of their official duties and should not be held criminally of civilly liable for such acts. **Note:** A child detained pursuant to the provisions on c. 94C § 36 shall not be considered to have been arrested or to have a criminal record for any purpose. Only a Departmental record of custody shall be made by the member(s) indicating the circumstances of the custody.

Non-Secure Detention

A juvenile in protective custody under MGL c. 111B, § 8, shall be held in accordance to the requirements specified for non-secure detention. These requirements are:

- The area where the juvenile is held is in an unlocked, multipurpose section, such as a report writing room or office;
- The space is in no way designed for residential use;
- The juvenile is held long enough to complete identification and processing, and then shall be released to a parent, guardian, legal custodian, other responsible adult;
- The juvenile is under continuous visual supervision until released; and
- At no time is the juvenile to be handcuffed to any stationary object.

Note: **A juvenile in protective custody shall not be placed in a cell.** A juvenile in protective custody may be handcuffed, but not to a stationary object, and shall not be considered in "secure detention".

Subject:	Number:
Protective Custody	**DET-10**

References: DET-09 Juvenile Detention;
TRF-14 Operating Under the Influence;
SP 850 Protective Custody;
M.G.L. c.111B;
M.G.L. c.111B, § 3;
M.G.L. c.111B, § 8;
M.G.L. c.111B, § 10;
M.G.L. c.111E;
M.G.L. c.111E, § 9A;
Alfano v. Lynch, 847 F.3d 71 (CA1 2017);
Comm. v. O'Brien, 434 Mass. 615 (2001);
Comm. v. O'Connor, 406 Mass. 112 (1989);
Comm. v. Tomes, 400 Mass. 23 (1987).

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**GEN-01**
Subject:	
Personal Appearance	

Policy

As the principal law enforcement agency within the Commonwealth of Massachusetts, members shall present an image of the highest standard, order, and professionalism to the public.

Members shall correct any deficiencies in their personal appearance, uniform, or equipment as soon as practicable, unless otherwise specified in this Order.

Jewelry

No jewelry, pins, necklaces, or bracelets of any kind shall be worn with the uniform. Exceptions, if conservative, are:

- Wristwatch;
- Medic Alert bracelet;
- Rings; and
- Necklaces worn discreetly beneath the shirt.

Note: Earrings shall not be worn while in uniform; however, conservative earrings may be worn by members in plainclothes assignments.

Members shall not display implants or facial/body piercing, while on duty or representing the Department. Note: In some instances, implants may be acceptable if a licensed medical practitioner requires the medical procedure and the procedure is performed under the medical practitioner's supervision.

Facial/body piercings include, but are not limited to:

- Piercing of the face, tongue, nasal septum, lips or lip plate; or
- The deliberate expansion of a healed fistula (hole in the skin) for wearing body-piercing jewelry; or
- The transdermal or microdermal implants.

Exception:
Members who are on undercover assignment may display facial or body piercings, when authorized by their Division Commander.

Hygiene and Oral Hygiene

Members' personal care shall conform to the highest personal hygiene standards.

Members, when in any uniform or representing the Department, shall ensure:

- Teeth will be clean and free of foreign debris;
- There is an appearance of a full set of teeth; and
- Missing or broken teeth and/or loose orthodontics shall be replaced or repaired as soon as possible.

Members shall not display dental/oral modifications to their teeth or mouth area while on duty or representing the Department. Note: In some instances, dental/oral modifications or procedures may be acceptable if a licensed dental or medical practitioner requires the medical procedure and the procedure is performed under their supervision.

Dental/oral modifications include, but are not limited to:

- Tongue splitting or bifurcation;
- Abnormal filing of the teeth; and
- Dental veneers or laminates ornamented with designs, jewels, initials, or any other decoration.

Cosmetics

Cosmetics, if worn, shall be:

- Subdued and blended to match the natural skin color; and
- Conservative.

No false eyelashes or unnaturally colored contact lenses shall be worn.

No fingernail polish of any color shall be used when in uniform.

Tattoos and Body Modifications

Members shall comply with General Order GEN-01A Tattoos and Body Modifications.

Hair

Hair shall:

- Be clean, neat, and well groomed;
- Not touch the top of the uniform shirt collar, at the back, when standing with the head in a normal posture;
- Not interfere with the wearing of any issued headgear; or
- Not be dyed or tinted in an exaggerated or unnatural color.

Subject: Personal Appearance	Number: GEN-01

Hair, continued

Note: Wigs or hairpieces may be worn if they conform to the above standards.

Males in Uniform:
Hair shall be:
- Either tapered or blocked at the back of the neck; and
- Tapered or blocked at the sides but may not touch the ears.

Sideburns shall be:
- Neatly trimmed and rectangular;
- Trimmed horizontally, at a right angle;
- Of even width; and
- No longer than the midpoint of the tragus of the ear.

Faces shall be clean shaven except:
- Members assigned undercover, and with the approval of the Unit/Section Commander; or
- Members with a temporary medical condition, verified by the State Police Surgeon.

Note: Members with mustaches, beards, or goatees shall not appear in uniform.

Females in Uniform:
- Hair may extend over, but not below, the bottom of the ear, nor more than two inches forward of the ear;
- Conservative ponytails, braids, hair buns, etc., may be used if secured to the head; and
- Inconspicuous hair aids that blend in with the hair may be used.

References

GEN-01A Tattoos and Body Modifications;
Rules & Regulations, Article 10;
MGL c. 22C, § 19;
MPAC: 22.2.5, 26.1.1;
Inturri v. City of Hartford, 2006 WL 231671 (2nd Cir. 2006).

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**GEN-01A**
Subject:	
Tattoos and Body Modifications	

Policy

Pursuant to GEN-01 Personal Appearance, members shall present an image of the highest standard, order, and professionalism to the public.

Members of the Department shall maintain their personal appearance to the highest standards possible and in conformance with GEN-01 Personal Appearance.

All Sworn Members

No sworn member of the Department shall have ANY tattoo, scarification or brand that is considered extremist.

Extremist tattoos, scarifications or brands are those affiliated with, depicting, and/or symbolizing extremist philosophies, organizations, or activities. Extremist philosophies, organizations, and activities are those which advocate racial, gender and/or ethnic hatred or intolerance; advocate, create, or engage in illegal discrimination based on race, color, gender, gender identity, sexual orientation, ethnicity, religion, or national origin; and/or advocate violence or other unlawful means of depriving individual rights under the U.S. Constitution, Federal, or State law.

For purposes of this policy, the above prohibition on *extremist* tattoos, scarifications or brands shall also include indecent, sexist and racist tattoos, scarifications or brands:

- *Indecent* tattoos, scarifications or brands are those that are grossly offensive to modesty, decency, or propriety; shock the moral sense because of their vulgar, filthy, or disgusting nature or tendency to incite lustful thought; or tend reasonably to corrupt morals or incite libidinous thoughts.
- *Sexist* tattoos, scarifications or brands are those that advocate a philosophy that degrades or demeans a person based on gender or gender identity, but that may not meet the same definition of "indecent."
- *Racist* tattoos, scarifications or brands are those that advocate a philosophy that degrades or demeans a person based on race, ethnicity, or national origin.

All Sworn Members, continued

No sworn member shall have a tattoo, scarification, or brand on his or her face, neck or hands (wrist to fingertips).

NOTE: This prohibition pertaining to face and hands does not apply to members who have:

- Permanent commitment band(s) on the hand(s); and/or
- Permanent eyeliner, eyebrows or lipstick, if the permanent color is conservative and compliments the complexion and uniform.

However, under no circumstances shall any sworn member be allowed to add ANY additional permanent markings to his or her face.

Effective June 22, 2020, no sworn member shall add any additional tattoo, scarification or brand, regardless of size, normally visible while on-duty in ANY authorized uniform or attire.

Applicants

All applicants seeking sworn appointment to the Department shall be screened during applicant processing to assess compliance with this General Order.

If an applicant is found to be in violation of this General Order, then the applicant may, at his or her sole discretion, have the non-compliant tattoo, branding, or body art, or visible portion thereof, removed at his or her own expense. If an applicant expresses a willingness to remove a non-compliant tattoo, branding, or body art, his or her application for appointment will be suspended until the removal process is completed and re-evaluated for compliance. Removal of any markings will not per se absolve the applicant of being deemed as having such affiliation or adherence to said philosophies, organizations or activities that may be apparent in any phase of the selection process.

No applicant shall add any additional tattoo, scarification or brand, regardless of size, normally visible while on-duty in ANY authorized uniform or attire**.**

Prior to appointment to the Massachusetts State Police Training Academy, any applicant who has tattoos/body art/brands/scarifications, normally visible while on-duty in **ANY** authorized uniform or attire, shall submit to the Division of Administrative Services / Human Resources Section for inclusion in the applicant's personnel file:

- An SP 802A Applicant Identification and Reporting of Tattoos/Body Art/Brands/Scarifications

Applicants, continued

The SP 802A must contain the following information:

- The date the tattoo/body art/brand/scarification was received;
- A description and photograph(s) of the respective tattoo/body art/brand/scarification; and
- The size and location of the tattoo/body art/brand/scarification on the member's body that is visible while wearing the Department uniform.

Body Modifications

Body modification to any area of the body that is visible while on-duty in ANY authorized uniform or attire is prohibited.

The use of gold, platinum or other dental veneers or caps for the purpose of ornamentation while on-duty is prohibited. Teeth, whether natural, capped, or veneer shall not be ornamented with designs, jewels, initials, etc.

Body piercing jewelry not concealed by any authorized uniform or approved attire while on-duty is prohibited with the exception of earrings worn in compliance with GEN-01 Personal Appearance.

- The wearing of any facial jewelry to include, but not limited to tongue piercings, lip piercings, nose piercings, brow piercings by any sworn member of the Department while on-duty is prohibited.

Exception: Members who are on undercover assignment may display facial or body piercings when authorized by their Division Commander.

References

GEN-01 Personal Appearance;
Rules and Regulations, Article 10;
SP802 Sworn Member Identification and Reporting of Not Previously Documented Tattoos/Body Art/Brands/Scarifications;
SP 802A Applicant Identification and Reporting of Tattoos/Body Art/Brands/Scarifications;
MPAC: 26.1.1.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**GEN-02**
Subject:	
Uniforms	

Policy

Members of the Department (members) shall maintain their personal appearance and uniforms at the highest standards possible.

Only equipment and apparel issued or authorized by the Department shall be carried or worn.

Members of the Department shall be issued required uniforms and equipment as required by their position to be worn in accordance with this policy. Uniforms and equipment shall be issued to members by the Section/Unit with oversight of said item(s) and an inventory of each item issued shall be maintained by the issuing entity.

Sworn Department members required to perform work in civilian clothing shall receive an annual clothing allowance in accordance with the Collective Bargaining Agreement for Unit 5A of the State Police Association of Massachusetts.

State Police Cadets shall wear the issued uniform in accordance with TRN-05 State Police Cadet Program and adhere to applicable sections of this policy related to uniform care and appearance.

Upon separation from service, or in accordance with Rules & Regulations, Department members shall return issued uniforms and equipment to the Supply Section.

Cruiser Operation

While operating Department vehicles, all members are required to wear the authorized uniform, appropriate business attire, or attire specifically related to their position.

Members shall display their badge of office while operating a Department vehicle. Exceptions may be allowed for:

- Members assigned to the Division of Investigative Services (DIS), Division of Homeland Security and Preparedness (DHS) or to other assignments where the member's identity should not be revealed as authorized by their Station/Section/Unit Commander.

Subject: Uniforms	Number: GEN-02

General

Supervisors are responsible for continuous line inspections to ensure that members under their control maintain a professional appearance and correctly wear the uniform.

Whenever two (2) or more members are gathered in the same location, the members shall dress the same as the Officer in Charge (OIC) or Senior
Trooper, or as otherwise ordered.

While in uniform, members shall not:

- Participate in social functions, unless authorized to do so by their Division Commander;
- Wear unauthorized or non-issued clothing, parts, medallions, ornaments, or other appurtenances;
- Wear personal headphone devices, earphone devices, or cellular phone headsets;
- Consume alcoholic beverages;
- Use tobacco in any form, smoke e-cigarettes or vape pens, chew gum, or have any foreign object protruding from the mouth when they are:
    - In view of the public; and/or
    - In formation.

Members shall not permit any non-member to wear any part(s) of any issued Massachusetts State Police uniform assigned to them.

Members shall not wear any part of the uniform while off-duty, unless authorized to do so.

Replacement of Uniforms or Equipment

When items are worn out, damaged, destroyed through normal use, or do not fit, members may turn in items to the Troop Clerk and requisition a replacement.

When items are damaged or destroyed through negligence or misuse, the member shall replace the item(s) at their own expense.

The Supply Section and/or Troop Clerk shall inspect issued uniform parts returned due to promotion or separation from service. Uniform parts that have useable life remaining may be reissued if in good working order/condition in accordance with normal issuance procedures.

Cleaning and Maintenance

- Boots, shoes, and leather shall be highly polished;
- Brass shall be clean and highly shined;
- Clothing items shall be clean, stain free, and pressed;
- Necessary alterations or repairs may be done through the Troop Clerk; and
- Whenever an occasion causes deficiencies in personal appearance, uniform, or equipment, members shall avail themselves of the first opportunity to correct the condition.

Riot Gear

All members, unless undercover, shall carry all issued riot gear in the trunk of their cruiser.

The OIC at a riot or disturbance may designate the following items as optional:

- Necktie and tie clasp, cross-strap, name tag, badge of office, whistle and chain, and gas mask; and/or
- Use of force equipment as defined in *UOF-04 Use of Force Equipment.*

Summer and Winter Uniform Dates

The Summer Uniform shall be worn from:

- April 15th through October 14th.

The Winter Uniform shall be worn from:

- October 15th through April 14th.
  Note: The Winter shirt is optional for thirty (30) days before and after this period.

Note: Staff Officers while in any uniform shall wear the garrison cover at all times.

Full Dress (Class "A") Uniform

The Class "A" Uniform is for ceremonial or dress occasions. It consists of:

- Long sleeve shirt;
- Necktie and tie clasp;
- Blouse;
- Breeches;
- Field boots;
- Duty belt with only the holster and firearm, ammunition case, baton ring, handcuff case, and the cross-strap;
- Appropriate cover (the garrison cover during winter for all members; the straw campaign cover during summer for all members, except Staff Officers who shall wear the garrison cover);
- Black or white gloves, when authorized; and
- Authorized ribbons and medals.

Sunglasses, keepers, and extra handcuffs shall not be worn with the Class "A" uniform.

For designated periods of mourning, a black badge shroud shall be worn around the badge of office.

Summer Field Service (Class "B") Uniform

- Straw campaign cover shall be worn with cord trimmed to an appropriate length (not knotted) and as follows:
  - *Troopers*: Silver hat badge and silver acorns;
  - *Non-Commissioned Officers*: Silver hat badge and silver acorns;
  - *Commissioned Officers*: Gold hat badge and gold acorns;
  - *Command Staff*: Garrison cover with gold hat badge, gold fretting, and glossy gold hat band with black leather straps removed;
- Short sleeve shirt, top button unbuttoned, no undergarments or jewelry visible;
- Slacks;
- Jump boots;
- Body Worn Camera;
- Garrison belt;
- Duty belt with keepers, holster and firearm, OC spray, handcuff case, baton ring, ammunition case, and other authorized equipment;
- Sweater (optional) tucked into slacks with badge on left chest, name tag on right chest;
- Issued outerwear (optional); and
- No ribbons or medals, except service ribbon.

If the long sleeve shirt or issued sweater is worn, a necktie and tie clasp shall be worn without the cross-strap.

Winter Field Service (Class "B") Uniform

- Garrison cover shall be worn with:
  - *Troopers:* Silver hat badge and black leather strap on front and back;
  - *Non-Commissioned Officers*: Silver hat badge and silver hat band on front with black leather straps removed;
  - *Commissioned Officers*: Gold hat badge and gold hat band on front with black leather straps removed;
  - *Command Staff*: Gold hat badge, gold fretting, and glossy gold hat band with black leather straps removed;
- Long sleeve shirt, completely buttoned, with necktie and tie clasp;
- Breeches;
- Field boots;
- Body worn camera;
- Garrison belt;
- Duty belt with cross-strap, keepers, holster and firearm, handcuff case, club ring, ammunition case, and other authorized equipment;
  - Cross-strap shall be worn diagonally across the wearer's front and back, secured directly in front of and behind the holster.
- Sweater (optional), tucked into breeches with cross strap removed and badge on left chest, name tag on right chest;
- Issued outerwear (optional);
- Black gloves and balaclava (optional); and
- No ribbons or medals, except service ribbon.

Knit caps shall not be worn with the Winter Field Service (Class "B") uniform.

Summer Field Service (Class "C") Uniform

- Straw campaign cover shall be worn with cord trimmed to an appropriate length (not knotted) and as follows:
  - *Troopers*: Silver hat badge and silver acorns;
  - *Non-Commissioned Officers*: Silver hat badge and silver acorns;
  - *Commissioned Officers*: Gold hat badge and gold acorns;
  - *Command Staff*: Garrison cover with gold hat badge, gold fretting, and glossy gold hat band with black leather straps removed;
- Short sleeve Super shirt, top button unbuttoned, no undergarments or jewelry visible;
  Or
- Armorskin ballistic vest carrier with short sleeve base shirt worn underneath, top button unbuttoned, no undergarments or jewelry visible;
- Class C Slacks;
- Jump boots;
- Body worn camera;
- Garrison belt;
- Duty belt with keepers, holster and firearm, handcuff case, club ring, ammunition case, and other authorized equipment;
- Sweater (optional) tucked into slacks with badge on left chest, name tag on right chest;
- Issued outerwear (optional); and
- No ribbons or medals, except service ribbon.

If the long sleeve Super shirt or issued sweater is worn, a necktie and tie clasp shall be worn without the cross-strap.

If the Armorskin and long sleeve base shirt and is worn, a necktie without tie clasp shall be worn tucked underneath the Armorskin without the cross-strap.

Specialty Uniforms

When authorized to do so by their Division Commander, members may wear specialty uniforms. Only members who are performing a specialized function shall wear specialty uniforms.

The Division Commander of Standards and Training, or designee, may revise the duty uniform of personnel assigned to the Academy.

Issued Uniform Parts and Equipment

The **Badge of Office** shall be:

- Prominently displayed by wearing it on the left breast area of the outer uniform garment.

The **Headgear badge** shall be:

- Worn on all campaign covers and garrison covers.

Collar insignias shall be:

- Worn on summer and winter shirts and the dress blouse only;
- Placed with the Commonwealth ornament on the right hand side;
- Placed with the troop designation ornament on the left hand side; and
- Placed one (1) inch back from the leading edge of the collar and centered between top and bottom.

Service chevrons may be:

- Worn, one (1) for every two (2) years of service; and
- Worn on the left sleeve of the blouse, pointing downward with the lowest chevron centered one and one-half (1 ½) inches above the semicircular cuff edging.
  Note: Service chevrons shall not be worn by Commissioned and Non-Commissioned Officers.

Non-Commissioned Officer stripes shall be:

- Worn on both sleeves of all shirts, (except Specialty Uniforms and/or BDU's – worn on the collar), the dress blouse and outer garments except traffic vest and rain jacket;
- Aligned so that the points of the stripes face upward;
- Positioned on the right sleeve so that the point of the highest stripe touches the bottom point of the MSP patch; and
- Positioned on the left sleeve to mirror the location of the stripes on the right sleeve.

Commissioned Officers Rank Insignia shall be:

- Worn on both shoulders of all Class B shirts, Class C Super shirts, the Armorskin ballistic carrier, the blouse, and outer garments, except traffic vest and rain jacket (Specialty Uniforms – worn on the collar); and
- For Class B, centered between the shoulder seam and shoulder strap
- For Class C Super Shirt, the rank insignia should be cut down to 1 ½ inch by 1 ½ inch and placed a ½ in from the edge of the shoulder seam (Please refer to Class C wear PowerPoint presentation found in Power DMS).
- For Armorskin Ballistic Carrier, the outside edge of the rank insignia should be placed on the edge of the inside seam of the shoulder strap (Please refer to Class C wear PowerPoint presentation found in Power DMS).

Issued Uniform Parts and Equipment, continued

Name tags shall be:

- Prominently displayed on all outer uniform garments, except rain jacket and high visibility safety apparel;
- Affixed to the lower seam edge running horizontally across the right breast and centered over the button of the shirt/blouse pocket; and
- Positioned to appear centered between the lapel edge and shoulder seam.

Tie clasps shall be:

- Worn on the tie, clipped to the shirt, and horizontally even with the name tag.

The **chain, key and whistle** shall be:

- Worn suspended from the right epaulet button and attached to the right breast pocket button on the blouse or shirt;
- Worn with the chain under the name tag; and
- Worn in the following order from the member's right: chain-key-whistle.

Issued use of force equipment, ammunition, handcuffs, and portable radio shall be:

- Carried and secured in appropriate cases on the duty belt.

The **rain jacket** shall be:

- Worn during inclement weather**,** high visibility side displayed (see *Issued High Visibility Safety Apparel* section of this General Order), except for solemn or ceremonial occasions, where the black side shall be displayed. Note: No rank insignia shall be worn on the rain jacket.

The **traffic vest**:

- See *Issued High Visibility Safety Apparel* section of this General Order. Note: No rank insignia shall be worn on the traffic vest.

Promotion Instructions

Prior to the effective date of promotion, members shall report to the Supply Section to be issued appropriate uniforms and gear related to said rank. Unless specifically detailed below, uniforms and uniform parts shall remain the same as the next highest rank.

All Ranks

Patrol Jackets

Both reversible patrol jackets should be returned to the Supply Section for an exchange or for application of new rank insignia in the appropriate location(s).

Staff Officers and Commissioned Officers

Rank Insignia

The following ranks will be issued the respective cloth and brass rank insignia:

- **Colonel:** Silver Eagle;
- **Lieutenant Colonel:** Silver Oak Leaf;
- **Major:** Gold Oak Leaf;
- **Detective Captain:** Double Silver Bars;
- **Captain:** Double Gold Bars;
- **Detective Lieutenant:** Single Silver Bar; and
- **Lieutenant:** Single Gold Bar.

Cloth Rank Insignia shall be:

- Sewn onto both shoulders of all uniform shirts, except Class C Base shirt; (positioning for Class B & C mentioned above already)

Brass Rank Insignia shall be worn on:

- Blue side of patrol jackets;
- Dress blouse; and
- Sweater.

Promotion Instructions, continued

Gold Braiding

Detective Lieutenants/Lieutenants will be issued a dress blouse with the appropriate gold braiding already affixed.

The following ranks will be issued additional gold braiding to be affixed to the sleeve of the lieutenant dress blouse, resulting in:

- **Colonel:** Four (4) rows of one-half (1/2) inch braiding affixed one-eight (1/8) inch from each other;
- **Lieutenant Colonel:** Three (3) rows of one-half (1/2) inch braiding affixed one-eight (1/8) inch from each other;
- **Major:** One-half (1/2) inch braiding, then one-quarter (1/4) inch braiding, then one-half (1/2) inch braiding affixed one-eight (1/8) inch from each other;
- **Detective Captain/Captain:** Two (2) rows of one-half (1/2) inch braiding affixed one-eight (1/8) inch from each other.

Detective Lieutenants/Lieutenants

Detective Lieutenants/Lieutenants will be issued the following:

Uniforms

- Dress Blouse with the appropriate gold braiding already affixed;
- Slacks and Breeches with two (2), one-half (1/2) inch blue braiding sewn along each pant leg; and
- Long and short sleeve shirts.

Gold Accessories

- Chain / handcuff key / whistle;
- Collar ornaments;
- Duty Belt brass; and
- Tie clasp.

Gold MSP Patches

All blue MSP patches should be removed from the current issue, except rain jacket, and replaced with the gold patches. Troop Clerks may be consulted for alteration locations.

Gold Reflective Tape for Riot Helmet:

- One (1) gold strip of tape is to be placed horizontally on the back of the helmet from rivet to rivet; and
- One (1) gold strip of tape is to be placed starting on the crown of the helmet downward to the front visor.

Sergeants

Sergeant will be issued the following:

Cloth Non-Commissioned Officer Stripes Rank Insignia with dark blue stripes and light blue background which shall be affixed accordingly:

- Sewn onto the dress blouse and onto all uniform shirts;
- Worn on both sleeves of dress blouse, and all shirts;
- Aligned so that the points of the stripes face upward;
- Positioned on the right sleeve so that the point of the highest stripe touches the bottom point of the MSP patch; and

Promotion Instructions, continued

- Positioned on the left sleeve so as to mirror the location of the stripes on the right sleeve.

  Note: Cloth Non-Commissioned Officer Rank Insignia with light blue stripes and **dark** blue background are for winter sweaters and patrol jackets only.

Silver Reflective Tape for Riot Helmet:

- One (1) silver strip of tape is to be placed horizontally on the back of the helmet from rivet to rivet; and
- One (1) silver strip of tape is to be placed starting on the crown of the helmet downward to the front visor.

Issued High Visibility Safety Apparel

High Visibility Safety Apparel is comprised of fluorescent colored background material that has retro-reflective applications affixed to it, thus providing the wearer with a high degree of visibility during both daylight and darkness.

The following Department issued apparel shall be considered high visibility safety apparel:

- High visibility yellow traffic test;
- Civilian traffic vest;
- Reversible Rain Jacket with high visibility yellow side displayed; and
- Reversible Patrol Jackets with high visibility yellow side displayed.

Department Employees (sworn and civilian) are advised that issued high visibility safety apparel shall be:

- Worn in accordance with current state and federal laws.

Specific clothing worn by certain sections of the Department may be considered high visibility safety apparel, only if the article of clothing has an American National Standards Institute-International Safety Equipment Association (ANSI/ISEA) certified label affixed to it.

The Department realizes that members performing motor vehicle stops have discretion when balancing their need to be visible to approaching traffic and their need to ensure proper patrol procedures/officer safety during the course of the motor vehicle stop.

Employees (sworn and civilian) are not required to wear high visibility safety apparel when:

- A member is performing a motor vehicle stop; or
- A civilian employee is performing functions away from the roadway and traffic areas.

However, members who choose not to wear high visibility safety apparel during motor vehicle stops shall:

- Remain vigilant and understand that they are less likely to be seen by approaching motor vehicle traffic particularly:
  - In darkness; or
  - In periods of diminished visibility due to inclement weather.

Issued High Visibility Safety Apparel, continued

Employees (sworn and civilian) wearing uniforms or plain clothes shall wear high visibility safety apparel during all hours and lighting conditions when engaged in the following activities:

- Directing traffic;
- At all road and highway motor vehicle crash scenes;
- When working at lane closures and obstructed roadways;
- On all road and highway work zones and construction details including moving details (excluding dignitary protection); and/or
- Special or significant events when ordered by the OIC.

Eye Wear

Members performing a line function and wearing prescription lenses shall have:

- Safety lenses; and
- Conservative and secure frames.

Sunglasses may be worn for outside assignments only, and shall be of a conservative style.

Department Issued Ribbons and Medals

While in Class "B" uniform, Department members who have attained ten (10) years of service shall be allowed to wear over the left breast pocket of the shirt:

- The Department issued Service Ribbon (blue/white/blue); and
- If applicable, one (1) gold star for each additional five (5) years of service to be inserted onto the white section of the ribbon.

Department issued ribbons and medals shall be worn on the Class "A" uniform over the left breast pocket of the blouse. However, if the member has military awards, the Department ribbons and medals shall be worn over the right breast pocket of the blouse.

Memorial pins, medallions, insignias, or other ornaments shall not be worn, unless authorized by the Colonel/Superintendent.

Military Ribbons and Medals

Awarded ribbons and medals issued by the U.S. Armed Forces may:

- Be worn or displayed, in military fashion, while in Class "A" uniform over the left breast pocket of the blouse.

No military ribbons or medals shall be worn or displayed while in Class "B" uniform.

Subject:	Number:
Uniforms	**GEN-02**

References

M.G.L. c. 22C, §19;
M.G.L. c. 149, § 6;
Massachusetts State Police Rules and Regulations Article 5; UOF-04 Use of Force Equipment;
Commonwealth of Massachusetts Division of Occupational Safety Department of Transportation Federal Highway Administration Manual on Uniform Traffic Control Devices;
American National Standards Institute-International Safety Equipment Association (ANSI/ISEA) 107 & 207 Standards;
MPAC 17.5.1, 22.2.5, 26.1.1, 41.3.4.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**GEN-04**
Subject:	
Military Courtesy	

Policy

The Department has been a paramilitary organization since its inception; the application of military courtesies shall continue to maintain this tradition.

Salutes

Salutes shall be given when members are both in uniform and covered, unless it would interfere with the performance of duty.

Salutes shall be given to a Staff Officer or a Commissioned Officer, and be smartly and promptly acknowledged by that member. In the case of Commissioned Officers, this rule shall only apply to members of superior rank.

Salutes shall also be given to the Governor, President and Vice President.

This policy shall also apply when meeting uniformed members of other police agencies and the Armed Forces.

Salutes in Formation

Members shall salute upon a command from the Commanding Officer when:

- In formation at a halt, the commands are "Attention", then "Present Arms" and the recovery command is "Order Arms"; and
- In a moving formation, the salute is only executed by the Commanding Officer leading the formation; the command for the formation is "Eyes Right" (or left), and then "Ready Front" as the salute.

Attention

Upon entering the office of the Colonel/Superintendent, a Lieutenant Colonel, or a Major, a member shall remove their cover and stand at attention.

Subject:	Number:
Military Courtesy	**GEN-04**

National Anthem

Members in uniform shall stand at attention and salute when the National Anthem is played:

- Facing the music (unless the National Flag is displayed); and
- Starting at the first note of the anthem, continuing to the last note.

If in civilian clothes, the right hand is placed over the heart in lieu of the salute.

National Flag

Unless it would interfere with the performance of duty, uniformed members wearing the appropriate cover, shall stand at attention facing the flag and salute when:

- It passes by on all public occasions, ceremonies, parades, etc. (The salute shall be given when the flag has arrived within a distance of six (6) paces and maintained until it has passed six (6) paces beyond); or
- It is carried into any building, room, or other place where members are present; or
- It is formally raised or lowered.

If in civilian clothes, the right hand is placed over the heart in lieu of the salute.

Pledge of Allegiance

Unless it would interfere with the performance of their duty, during the Pledge of Allegiance members shall:

- Stand at attention facing the flag and salute when in uniform wearing the appropriate cover; or
- Stand at attention facing the flag and place their right hand over their heart if in civilian clothes.

Display of Flags

The Flags of the United States and the Commonwealth shall be flown at all Department facilities. The National Colors shall be flown on the flag's own right, (on the right as facing the street), and slightly higher than the Commonwealth Flag.

Flags shall be flown:

- Every day when the weather permits; and
- At night if they are directly illuminated

The National Flag shall be flown at half-staff in honor of a member who dies while in the line of duty, from the notification of death until dusk of the day of interment.

Display of Flags, continued

The Flag of the Commonwealth shall be flown at half-staff when:

- The National Flag is at half-staff;
- As ordered by the Governor; or
- As ordered by the Office of the Superintendent.

On Memorial Day, the flags should be flown at half-staff until noon, and then raised.

To display flags at half-staff, the flags should be hoisted to the peak, and then lowered to half-staff.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**GEN-04A**
Subject:	
Ceremonial Tributes	

Policy

The protocols identified within this policy shall be adhered to during ceremonial tributes honoring Department members or when attending tributes with other agencies.

Request Procedure and Authorization

The Colonel/Superintendent shall authorize final approval for all Department tributes and requests from outside agencies. The Division of Field Services shall handle implementation, unless otherwise ordered.

Ceremonial Tributes

The Department may provide the following as determined by the Colonel/Superintendent:

Line of Duty Death

- Wake – Organized police walk-by, honor guard and/or color guard detail;
- Drill and Ceremonial Unit;
- Rifle Salute;
- Mounted Unit;
- Motorcycles;
- Air Wing;
- Vocalist and bugler(s);
- Department Pipes & Drums;
- Classmates of the Deceased;
- Specialty Unit/Team to which the member belonged;
- Minimum of forty (40) members; and
- All available members of the Command Staff.

Off-Duty Death

- Wake – Honor guard at wake consisting of member's troop/section;
- Drill and Ceremonial Unit;
- Motorcycles;
- Classmates of the Deceased;

Ceremonial Tributes, continued

- Vocalist, bugler and piper;
- Specialty Unit/Team to which the member belonged;
- Minimum of twenty (20) members; and
- Division Commanders or Designees.

Death of Immediate Family Member of an Active Member (spouse, child, brother, sister, parent of member or spouse)

- Four (4) members, provided for by the member's Station/Section/Unit, to cover calling hours, funeral detail, and the procession.

Retired Member(s)

- Two (2) members to be provided by the Division of Field Services to cover calling hours, funeral detail, and procession.

Active Public Safety Officers

The Colonel/Superintendent shall determine any ceremonial tributes provided for active public safety officers killed in the line of duty.

Funeral Attendance

The Department shall attempt to allow as many on-duty members as possible to attend the calling hours and funeral services of an active member.

Members to attend calling hours and funeral services in uniform shall:

- Wear the appropriate uniform-of-the-day as indicated on calling hours and funeral services announcements;
- Be authorized, when attending off-duty, to wear the uniform-of-the-day as indicated on calling hours and funeral services announcements; and
- While inside a funeral home or church carry their headgear under their left upper arm, unless directed otherwise or when participating as a member in the honor guard.

Honor Guard

Details at funeral homes should consist of at least four (4) members. The senior member should coordinate with the family liaison. Members shall wear the class "A" uniform, with a black badge shroud and white gloves, unless otherwise directed.

Funeral Processions

Upon leaving the funeral home or church, members should:

- Cover and form two (2) lines along the path where the casket is to be carried;
- The formation shall start at the funeral home or church and end at the hearse; and
- A proper interval shall be maintained between members.

Badge Shrouds

As designated by the Colonel/Superintendent, black badge shrouds shall be worn for thirty (30) days by all members in honor of an active member who dies in the line of duty.

Black badge shrouds shall be worn by all members in honor of an active member who dies off duty, from the date of the death notification until the interment.

Black badge shrouds shall be worn by uniformed members while appearing at a funeral or memorial service for active or retired members.

Funeral Escorts

Department vehicles escorting or following the funeral procession shall:

- Be operated at a speed consistent with that of the hearse and far enough ahead of the procession to control traffic; and
- Have all the emergency warning lights activated and left on during the entire escort.

Members assigned to traffic control duties where the funeral procession is passing by shall:

- If conditions allow, stand at attention and render the hand salute while the hearse is passing.

If the escort terminates at the entrance to a cemetery, church, or funeral home, the escorting members shall:

- Stand at attention in two (2) lines, face each other; and
- Render the hand salute until the hearse has passed by.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**GEN-05**
Subject:	
Communicable Diseases	

Policy

The Department shall provide its employees with equipment and information on communicable diseases to prevent exposure to dangerous and life-threatening diseases.

For the purpose of this policy only, the term employee shall refer to both sworn and civilian members of the Department.

Definitions

Airborne Exposure: Contact with bacteria, virus, chemical, smoke, or any foreign particle suspended in the environment.

Bodily Fluid: Liquid secretions such as blood, semen, vaginal secretions, saliva, vomit, urine, and feces.

Communicable Disease: Infectious illnesses and viruses that are transmitted through contact with bodily fluids, tissue, or breath of an infected individual.

Unprotected Exposure: Any bodily fluid or tissue that comes into direct contact with a mucous membrane (e.g., eyes, nose, and mouth) or non-intact skin (e.g., cuts, chapped skin). This includes a bite from a human or animal.

Communicable Disease Prevention

All employees should assume that all persons are potential carriers of communicable disease.

When coming into contact with people or evidence where the transfer of bodily fluids is a possibility, employees should wear protective clothing and equipment to minimize their exposure to disease. This includes:

- No eating, drinking, or smoking at a scene where bodily fluids are present;
- Wear disposable gloves when administering first aid or handling anything that has been exposed to bodily fluids (double gloves should be used, if necessary);
- Wear a protective mask, eye wear, and coveralls if available, in situations where bodily fluids may come into contact with the employee;
- Use the issued plastic mouth piece or other barrier resuscitation device when performing CPR;

Communicable Disease Prevention, continued

- Use extra care when handling contaminated sharp objects (e.g., wear protective gloves when conducting a search, or when handling sharp objects);
- Use a flashlight or baton to conduct an initial sweep of areas where sharp objects may be hidden;
- For transport or storage, place hypodermic needles in leak proof, rigid, puncture-resistant, shatterproof containers (needles should not be recapped, bent, broken or removed from the syringe); and
- All employees assigned to the Mass State Police Crime Lab (MSPCL) involved in the collection and handling of evidence shall follow Communicable Disease Prevention procedures identified in the current version of the Laboratory Safety Manual.

Disinfection Guidelines

If…	Then
Any unprotected skin surface comes in contact with bodily fluids	• Immediately and thoroughly wash the affected area with hot running water and soap for at least fifteen (15) seconds before rinsing and drying; • Use alcohol or waterless antiseptic hand cleaning gel when soap and water is unavailable; • Hand lotion should be applied after disinfection to prevent chapping and to seal cracks and cuts on the skin; and • When necessary, report to a medical facility for an examination or treatment.
You are wearing disposable gloves that come in contact with bodily fluids.	• Thoroughly rinse the glove before removing; and • Hands and forearms should then be washed as described above.
Uniform or clothing comes in contact with bodily fluid.	• Remove the uniform/clothing as soon as practical; • Place the contaminated uniform/clothing in a paper bag; • Any contaminated skin area should be cleaned as described above; and • Uniforms/clothing should be marked as contaminated and cleaned by: o Laundering in the usual manner; o Turning into the Supply Clerk for an exchange; or o Disposing according to the State Sanitary Code.

Disinfection Guidelines, continued

If…	Then
A Department vehicle becomes contaminated with bodily fluids.	• The Troop Supply Clerk shall arrange for a complete cleaning and disinfection, as soon as possible.

Non-disposable equipment becomes contaminated with bodily fluids.	• Wear protective clothing when cleaning;
	• Prepare a cleaning solution containing:
	  ○ One (1) part bleach to ten (10) parts water; or
	  ○ A fungicide or a micro bacterial disinfectant.
	• Wipe excess bodily fluids with disposable absorbent material;
	• Clean equipment with the prepared solution or disinfectant;
	• Dispose of the cleaning material according to the State Sanitary Code; and
	• Follow manufacturer's guidelines for proper disinfection/cleaning procedures.

Disposable equipment, (such as cleaning materials) contaminated with bodily fluids.	• Bag and dispose of according to the State Sanitary Code.
Evidence contaminated with bodily fluids is recovered.	• Place in paper bags and clearly mark as contaminated; • Allow items to dry out; • Take additional precautions as necessary; and • Consult with Crime Services Section for proper disinfection/handling procedures.

Transport and Custody

When transporting an individual who has bodily fluids on their person or has stated that they have a communicable disease:

Position	Duties
Members shall:	• Take all precautions to minimize the possibility of exposure to the bodily fluids; • Administer necessary first aid; • Transport this individual in a separate vehicle from other people; and • Notify the Desk Officer.
Desk Officers shall:	• Appropriately isolate the person; • Notify the Troop Duty Officer; and • Document the incident in the Daily Administrative Journal.

Reporting Unprotected Exposures

Members who have had an unprotected exposure while on duty should seek immediate treatment at an emergency room. Larger hospitals and teaching hospitals are often better able to assist with potential exposures.

The exposure shall be treated as an on-duty injury, and documented under the guidelines of ADM-11B Injury Reporting and Leave. In addition, a Department of Public Health Unprotected Exposure Form shall be filled out to document the exposure and:

- Taken to the medical facility where the member(s) is being treated, and
- E-mailed to the Health Unit at Healthandfitnessunit@pol.state.ma.us.

All employees assigned to the MSPCL involved in the collection and handling of evidence shall follow the exposure procedures identified in the current version of the Laboratory Safety Manual.

Department civilian employees shall seek guidance from their immediate supervisors who shall follow the procedures for sworn members.

Supplies

All Department cruisers and/or facilities should be stocked with the following communicable disease control supplies:

- Disposable and protective gloves;
- Puncture resistant containers and plastic evidence bags;
- Barrier resuscitation equipment, goggles, and masks;
- Liquid germicidal cleaner;
- Disposable towelettes with 70% isopropyl alcohol; and
- Waterproof bandages.

Health Unit Responsibilities

The Health Unit shall:

- Advise members about communicable disease and infection control matters;
- Conduct training pertaining to communicable disease and infection control matters;
- Distribute protective clothing and equipment; and
- Develop guidelines for the use of the equipment and providing care to the public.

Responsibilities

Position	Duties
Members	• Ensure that all assigned medical supplies are properly maintained; • Keep disposable and protective gloves readily available and easily accessible; • When an on-duty incident results in an unprotected exposure, notify the Desk Officer and follow the guidelines in this policy to minimize the risk of infection; and • No member shall refuse to handle or arrest any person.
Desk Officers	• Notify the Troop Duty Officer; and • Document the incident in the Daily Administrative Journal (DAJ).
Troop Duty Officer	• Ensure that any employee who has an unprotected exposure while on-duty receives proper first aid and medical treatment; • Assign a supervisor to investigate the exposure; • Document the incident in the DAJ; and • Ensure Notice of Injury Report is submitted forthwith per ADM-11B.

Commanding Officers	• Ensure that communicable disease control supplies are made readily available to all members of their Troop/Section/Unit;
	• In the case of an on-duty unprotected exposure, ensure that the employee receives:
	  ○ Assistance in reporting the exposure;
	  ○ Continued testing for evidence of infection; and
	  ○ Any emotional assistance or counseling as required.
	• Contact the District Attorney to ascertain if criminal charges are appropriate for intentional exposures.

References

The Ryan White Comprehensive AIDS Resources Emergency Act (Pub. L. 101-381);
OSHA Final Standard on Bloodborne Diseases 29 CFR 1910.1030;
105 CMR 170-172;
Massachusetts Department of Public Health Unprotected Exposure Form
MGL c.111, s.111C;
105 CMR 480.00;
Massachusetts State Police Crime Lab SAFE Safety Manual ID:3550 Revision 6 Issued: 9/29/20.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**GEN-06**

Subject:

Drug Testing

Policy

In order to ensure public safety and promote public trust, it is the policy of the Department to maintain a drug-free work environment.

Purpose

The following compelling reasons justify the use of drug testing:

- **Public Trust**: Members who are sworn to enforce the law cannot be deemed to be above the law;
- **Public Safety**: The public expects members to have both the physical stamina and psychological stability to properly assume and perform required duties at all times;
- **Potential for Corruption**: Contact with controlled substances and people associated with them exposes members to increased opportunities for corruption;
- **Presentation of Credible Testimony**: A member who illegally uses or abuses drugs would be subject to impeachment through proof or an admission that they violated the law;
- **Morale and Safety in the Workplace**: Every member has the right to be secure in the knowledge that all members are capable of acting in a safe and effective manner; and
- **Loss of Productivity**: The use of controlled substances, and other forms of drug abuse, seriously impair physical and mental health and result in reduced job performance.

Scope

This Drug Testing policy applies to all sworn members of the Department.

Civilian employees may refer to the Code of Conduct or Commonwealth Employment Standards found in their respective collective bargaining agreement.

Medication Notification

All members shall notify their immediate supervisor when required to use medication that has the potential to impair their job performance.

- The member shall inform his/her supervisor of the known side effects of such medication and the prescribed period of use, and shall provide documentation of same;
- The supervisor shall document this information through the use of an internal memorandum to the appropriate Division Commander/Manager and shall send a copy to the Occupational Health Unit for review by the State Police Surgeon; and
- The member may be temporarily reassigned other duties, if appropriate.

Subject:	Number:
Drug Testing	**GEN-06**

Prohibited Activity

Members are prohibited from:

- Illegally possessing any controlled substance, under either state or federal laws;
- Ingesting any unlawful/dangerous drug under either state or federal laws; and
- Ingesting any controlled substance, unless prescribed by a licensed medical practitioner and deemed legal under state or federal law.

Sanctions

Discipline for members found to be in violation of this Drug Testing policy shall be in accordance with Article 37 of the State Police Association of Massachusetts (SPAM) Collective Bargaining Agreement, the Rules and Regulations for the governance of the State Police, and MGL c. 22C.

Members who refuse to be tested when so ordered, or refuse to enter an Employee Assistance Program or Rehabilitation Program after a positive test, are subject to termination.

Drug Testing Program

Consistent with this policy, the Department has implemented a drug testing program for sworn members consisting of:

- Drug testing based on reasonable suspicion;
- Random drug testing;
- Post incident drug testing; and
- Annual/biennial physical drug testing.

Employees on extended leave may be subject to drug testing upon their return to service as determined by the Colonel/Superintendent.

Note: The terms “reasonable,” “random,” and “post incident” are defined consistent with Article 37 of the SPAM Collective Bargaining Agreement and all drug testing procedures shall be conducted in accordance with this article.

All drug testing methodologies shall be performed under the U.S. Department of Health and Human Services’ Mandatory Guidelines for Federal Workplace Drug Testing.

References

MGL c. 22C;
Article 37 SPAM Collective Bargaining Agreement;
Rules & Regulations 5.10.2;
ADM-11E Extended Leaves;
Substance Abuse and Mental Health Services Administration’s Mandatory Guidelines for Federal Workplace Drug Testing (https://www.samhsa.gov/workplace/resources).

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**GEN-07**

Subject:

Automated External Defibrillators

Policy

The Department maintains Automated External Defibrillators (AED) to help save lives. Only Department members trained in the use of AED's may operate them.

Definitions

Automated External Defibrillator (AED): An electronic device that when used may:

- Radically reduce the occurrence of disability and death associated with cardiac emergencies through:
  1) An analysis of the heart's rythm; and
  2) If necessary, administration of an electrical shock.

The supervisor of the Health and Fitness Unit shall have oversight of AED training, maintenance, and the creation of a standard operating procedure.

Care and Maintenance

Members shall:

- Follow AED procedures prescribed by the Health and Fitness Unit; and
- Ensure AEDs are not stored in unattended vehicles for any duration, where extreme temperature fluctuations may damage the device pads.

Responsibilities for Stations/ Sections with AED

AEDs are considered permanently assigned equipment to the Station/Section. Commanding Officers shall:

- Ensure annually that each device is accounted for according to ADM-30 Asset Management;
- Contact the Health and Fitness Unit for repairs, parts, batteries, or other AED associated supplies as needed if applicable; and
- Monitor AEDs on at least a monthly basis to ensure they are in working order (including checking expiration of pads and battery function)

Subject: Automated External Defibrillators	Number: GEN-07

AED Utilization

AEDs shall only be utilized by members who are trained. Members who possess AED's shall have a copy of the Health and Fitness Unit's SOP regarding use, maintenance, and reporting procedures. Follow manufacturer's recommendations for usage and American Heart Association (AHA) protocols.

Each time an AED is utilized to monitor and/or shock an apparent victim of a cardiac arrest the following procedures shall be adhered to:

Position	Duties
Utilizing Member	• Advise the Desk Officer of AED utilization; and • Before securing from their shift, complete and forward the SP 600 AED Utilization Reporting Form to the Health Unit.
Station Desk Officer	• Document the AED utilization as a Medical Assist into the Daily Administrative Journal; • Do not include the patient name or other identifiers within the entry; and • Provide the incident number to the member who utilized the AED.
Supervisor of the Health Unit	• Ensure AED protocols were followed; and • Review SP 600 AED Utilization Reporting Form.

References:
MGL c.111, § 201;
MGL c.112, § 12V ½;
105 CMR 171.180;
105 CMR 171.225;
ADM-30 Asset Management;
SP600 – AED Utilization Reporting Form.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**GEN-08**
Subject:	
Ride-Along/Observer	

Policy

The Department may allow approved ride-along/observers to accompany on-duty sworn members for educational purposes.

Requesting Permission to Observe

Requests for an observer(s) to accompany an on-duty sworn member shall be made in writing to the Troop/Section/Unit Commander and detail each observer's:

- Full name;
- Date of birth;
- Address;
- Social Security Number;
- Organization affiliation (if any);
- Date(s) of observation requested;
- Troop/Section/Unit to be observed; and
- Any special considerations (e.g. request to record, request to carry firearm).

The above information shall be forwarded via a SP 629 Massachusetts State Police Ride-Along/Observers Request and Release Form to the appropriate Division Commander. All requests for ride-along/observers and accompanying forms shall be maintained by the Division Commander's Office.

Media Requests

Requests for a ride-along for media representatives shall be referred to and approved by Commanding Officer of Media Relations.

Responsibilities

Position	Duties
Troop/Section/ Unit Commander	• Ensure a background check (including CORI) is conducted on any observer before approving any ride-along/observation; • Approve or deny the request; • Forward any SP 629 to their Division Commander; • Consult with Media Relations, if appropriate; • If approval has been granted, then assign a sworn member to handle the ride-along/observation duty; • Ensure appropriate safety precautions are taken to minimize risk and to ensure the well-being of the observer (e.g. require ballistic vest to be worn); and • Detail any conditions the observer and/or assigned sworn member shall follow.
Supervisor	• Ensure adequate scheduled staffing is available; • Ensure appropriate safety precautions are taken to minimize risk and ensure well-being of the observer; • Ensure any directives by the Troop/Section/ Unit Commander are adhered to; • Investigate any issues that may arise from an observation assignment per Department policies; and • Provide a summary of the concluded assignment to the Troop/Section/Unit Commander.
Sworn Member	• Shall conduct themselves in a professional manner; • Adhere to mandates of SUP-03 Media Relations relative to Department operations, administration and individual rights; • Carefully monitor the assigned observer(s); • Immediately report to their supervisor any injuries or issues regarding the observer(s); • Comply with directives issued by the Troop/ Section/Unit Commander; and • Provide a summary of the concluded assignment to their supervisor.

Subject: Ride-Along/Observer	Number: GEN-08

Responsibilities, continued

Position	Duties
Observer	• Sign appropriate forms as required by the Department's Legal Section; • Obey all commands and safety directives issued by the escorting sworn member; • Shall wear seatbelts while traveling in state owned vehicles; and • Agree to not electronically record the observation unless prior written approval is granted by the Troop/Section/Unit Commander and Media Relations. Note: Firearms shall not be carried, unless they are a law enforcement officer and the Troop/Section/Unit Commander has specifically approved this request.

References

Executive Order No. 241 Use Of Seat Belts By State Employees;
SUP-03 Media Relations;
SP 629 Massachusetts State Police Ride-Along/Observers Request and Release Form.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**INV-01**
Subject:	
Criminal Investigations	

Policy

Investigations shall be conducted on all matters of a criminal nature that fall within the jurisdiction of the Department.

Criminal Investigation

All members assigned to investigate a crime and/or criminal activity shall:

- Be responsible for the thorough and methodical investigation of assigned cases; and
- Continue the investigation until the case is:
  - Solved or otherwise closed, or
  - Until it appears that further investigation would be of no significant value;
- Comply with applicable Constitutional requirements, state and federal laws, Department policies and current case law when conducting criminal investigations that may include, but not be limited to:
  - Interviews, including field interviews;
  - Interrogations; and
  - Confessions/Admissions;
- Ensure specifically that applicable rights including, but not limited to, Miranda, access to counsel and the six hour safe-harbor rule, are applied when required in accordance with state and federal laws as well as established case law. The investigator shall explain these rights to the suspect as required by the investigation and documented by the investigator as applicable;
- Ensure that interviews and interrogations conducted by members include the administration to subjects/suspects of Miranda rights in accordance with state and federal laws as well as established case law, document the administration of the rights and, when practicable, utilize the SP-124 Miranda Rights Warning & Waiver form, Miranda rights administration is required for custodial interrogations;
- Understand and apply the provisions of Commonwealth v. Hipolito Rosario, 422 Mass. 48 (1996), regarding the six-hour safe harbor rule as they relate to the right to arraignment without delay and custodial interrogations, including but not limited to:
  - Statements shall be taken from a defendant within six hours of arrest, or at any time if the defendant makes an informed and voluntary written or recorded waiver of their right to be arraigned without unreasonable delay.
  - The period of safe harbor questioning commences on arrest and concludes six hours later without regard to when court is in session, except:
    - If the defendant is incapacitated upon arrest because of a self-induced disability (e.g., consumption of drugs), the six-hour period commences only when the disability terminates; or

Criminal Investigation, continued

  - If interrogation during the six-hour period is not possible or must be suspended for reasons not attributable to the police, such as a natural disaster or emergency, the six-hour period should be tolled appropriately.
- It is most important to recognize that, but for the exceptions just noted, the period of safe harbor questioning commences on arrest and concludes six hours later without regard to when court is in session.

- Immediately inform a detainee of an attorney's attempt to reach them and to immediately relay the attorney's message to them, including, when applicable, a message advising them not to talk to investigators. An entry into the Daily Administrative Journal (DAJ) or investigative record shall document the name of the member receiving the call, the name of the calling counsel including their Board of Bar Overseers (BBO) number and the name of the member delivering the message. (*Commonwealth v. McNulty,* 458 Mass. 305);
- Utilize audio and/or video recording of interviews and interrogations where practicable;
- Record interviews and interrogations when using interpreter services, where practicable (*Commonwealth v. Glenis A. Adonsoto 475 Mass. 497*); and
- Comply with the requirements of the member's Division in processing subjects arrested with/without a warrant to include a written report for all subjects arrested.

Arrests With/Without Warrant

Members conducting an arrest based upon a warrant shall ensure:

- Confirmation of the warrant prior to arrest in accordance with DET-01 Warrant Management;
- Notification to the barracks of jurisdiction of arrest;
- Documentation of the arrest in the DAJ or ACISS to include the assignment of an incident/case number;
- Transport to the barracks or court of jurisdiction;
- Give a true copy of the warrant to a detainee who requests a copy within six (6) hours;
- Process the arrest in accordance with Department policy; and
- Completion of a written incident report documenting the arrest.

Members conducting an arrest without a warrant shall ensure:

- Probable cause for arrest is established prior to custody;
- The detainee is advised of the arrest charge(s);
- Notification to the barracks of jurisdiction of arrest;
- Documentation of the arrest in the DAJ or ACISS to include the assignment of an incident/case number;
- Transport to the barracks or court of jurisdiction;
- Process the arrest in accordance with Department policy; and
- Completion of a written incident report documenting the arrest.

Alternatives to Arrest

Alternatives to arrest may include citations, summonses, informal resolution, warnings or referral to other agencies. Discretion to arrest or not to arrest may be guided by a totality of the circumstances articulable by the member exercising an arrest alternative. Enforcement of criminal and/or civil law shall be guided by Department policy and applicable state and federal laws.

- Circumstances where alternatives to arrest may be appropriate include, but are not limited to:
  - Arrest may aggravate community conflict or precipitate serious disorder;
  - Urgent public emergency or more serious crime necessitating immediate resource allocation/response;
  - Minor offenses where a lesser discretionary method may provide enforcement and documentation of incident(s); and
  - Medical emergencies.

Search & Seizure

Search and seizure of persons/places/objects without a warrant shall be guided by Department policy, state and federal laws, Constitutional law and current case law. This may include, but not be limited to:

- Search by consent;
- Stop and frisk of person(s);
- Motor vehicle search;
- Crime scene(s);
- Exigent circumstances;
- Inventory searches of persons/vehicles/property; and
- Other situations authorized by state and federal constitutional provisions, including but not limited to;
  - Abandoned property;
  - Open field doctrine;
  - Plain view; and
  - Search incident to arrest.

Division of Investigative Services / Division of Homeland Security and Preparedness

The Division of Investigative Services (DIS) and the Division of Homeland Security and Preparedness (DHS) shall investigate crime and/or criminal activity as determined by the Colonel/Superintendent, District Attorney or Attorney General and in accordance with their section/unit standard operating procedure (SOP).

Cases Involving Human Death

The District Attorney, upon notification of a death, directs and controls the criminal investigation, in conjunction with the law enforcement agency of jurisdiction. (M.G.L. c.38 s.4)

Criminal Investigations by Division of Field Services Members

Members assigned to the Division of Field Services may initiate criminal investigations, if warranted, in situations where criminal activity is occurring.

In cases where DFS members encounter a situation that necessitates some form of investigation, members may conduct a preliminary investigation concerning those offenses referred to or within the jurisdiction of the Department.

Members, or their supervisors, shall immediately notify through prescribed channels, the appropriate DIS section/unit or DHS section/unit when:

- Circumstances existing at the scene of the incident/offense require the application of specialized investigative techniques; and/or
- When the demands placed upon the responding member clearly exceed the scope of their investigative authority or abilities.

The Troop Duty Officer may notify the on-call person of each DIS/DHS Section/Unit for immediate assistance utilizing the on-call schedule which shall be posted to PowerDMS Documents/Calendars prior to the start of each month by each Section/Unit commander.

Criminal Investigations

<u>The first member arriving at a crime scene shall:</u>

- Make scene safety the first priority;
- Initiate medical services if needed;
- Secure and preserve the integrity of the crime scene;
- Conduct a preliminary investigation:
- Relinquish their responsibility only when directed by a supervisor or to the designated DIS/DHS investigator assigned to conduct the criminal investigation.

<u>Preliminary investigative steps may include:</u>

- Determining if a crime has been committed;
- Maintaining and protecting the crime scene;
- Observing and recording all conditions, events and remarks;
- Arrange for the collection of evidence, ensuring that evidence is not lost, destroyed, or altered in such a manner as to eliminate its probative value pending the arrival of crime scene/evidence technicians;
  - Do not move or touch physical evidence unless absolutely necessary, to ensure its preservation;
  - If physical evidence is moved, a notation shall be made of its exact location and position at the scene.
- Locating, identifying and interviewing the complainant and witnesses;
- Witnesses shall be interviewed:
  - As soon as possible and in a quiet environment, where practicable; and
- Separately to ensure independent statements; and
- Identifying, locating and interviewing/interrogating suspect(s).

Performing other duties necessary to build a solid foundation for follow-up investigators.

Criminal Investigations, continued

If the perpetrator(s)/suspect(s) has left the scene, pertinent information shall be broadcast, as soon as is practicable, utilizing all means necessary. The member(s) conducting the preliminary investigation should not rely solely on their memory, but should make field notes of all pertinent information. These notes may be subject to discovery in any criminal or civil matter, and may be subject to the Massachusetts Public Records Law, M.G.L. c. 66, § 10.

At a minimum, the following information should be recorded:

- Date and time of arrival at scene;
- Weather conditions and visibility;
- Exact location, to include addresses, distance measurements, and/or latitude/longitude when possible;
- Approximate time of the commission of the crime, when it was discovered, and by whom;
- Identity, if possible, or obtain the best available description of the criminal suspect(s);
- Description of any vehicle(s) used by suspect(s);
- Information concerning any physical evidence discovered;
- Name, address of complainant, victim and/or witnesses;
- Identity of other law enforcement officers or civilians present;
- Results of any interviews conducted and statements taken from complainant, victim and/or witnesses; and
- Any other information which may be useful in the apprehension of the perpetrator(s) and subsequent prosecution.

The member conducting the investigation shall complete a written report of the incident.

Follow-up Investigative Steps

If necessary, at a minimum, investigating officers should consider the following step(s) in order to bring the criminal investigation to a close:

- Reviewing and analyzing all previous reports prepared in the preliminary phase, departmental records, and results from laboratory examinations;
- Conducting additional interviews and interrogations;
- Seeking additional information (from other law enforcement officers, informants, etc.);
- Planning, organizing, conducting searches, and collecting physical evidence;
- Conducting search warrants in accordance with applicable Department policy, M.G.L. and current applicable case law;
- Identifying and apprehending suspects;
- Determining involvement of suspects in other crimes;
- Checking suspects' criminal histories;
- Preparing a written report documenting investigative steps undertaken; and
- Preparing cases, to include all required reports, for court presentation.

Victim/Witness Assistance

The rights of victim(s)/witness(es) of crimes shall be guided by state and federal laws as well as the Commonwealth's Bill of Rights which can be accessed at: https://malegislature.gov/Laws/GeneralLaws/PartIII/TitleIV/Chapter258B.

To the extent possible, the confidentiality of victims/witnesses and their role in case development, consistent with applicable law, shall be prioritized by investigating member(s).

Additionally, the Department shall provide appropriate assistance to victims/witnesses who have been threatened or who, in the judgment of the Department, express specific, credible reasons for fearing intimidation or further victimization. This may include seeking guidance from and/or referral to the Victim/Witness advocate of the Attorney General's Office or the District Attorney's Office assigned to the case.

Most Victim/Witness services are provided by the Attorney General's Office or the District Attorney's Office. However, nothing prevents a member of the Department from providing victim/witness assistance during the preliminary investigation including:

- Providing referral information verbally or in writing to the victim/witness about applicable services, e.g., medical attention and victim advocacy;
- Advising the victim/witness about what to do if the suspect or the suspect's companions or family threatens or otherwise intimidates them;
- Informing victims/witnesses about the case number and subsequent steps in the processing of the case;
- Providing a telephone number that the victim/witness may call to report additional information about the case or to receive information about the status of the case; and
- Providing notification to the victim/witness of the suspect(s) arrest, the charges, the suspect's custody status and changes thereto.

Victim/witness assistance may be provided by a member of the Department during the follow-up investigation including:

- Re-contacting the victim/witness periodically to determine whether needs are being met, if in the opinion of the agency, the impact of a crime on a victim/witness has been unusually severe and has triggered above-average need for victim/witness assistance;
- Explaining to victims/witnesses the procedures involved in the prosecution of their cases and their role in those procedures, if not an endangerment to the successful prosecution of the case;

Victim/Witness Assistance, continued

- Scheduling line-ups, interviews, and other required appearances at the convenience of the victim/witness and, at the option of the agency, providing transportation, if feasible; and
- Returning promptly victim/witness property taken as evidence (except for contraband, disputed property, and weapons used in the course of the crime), where permitted by law or rules of evidence if feasible.

Operation Plans, Documentation & Reports

All investigative activities, including actions taken, shall be documented in an investigative report or application for legal process. This includes, but is not limited to; surveillance, execution of search/arrest warrants, undercover and/or confidential informant purchases of illegal narcotics, decoy operations, or interviews, as well as information obtained as a result of said actions.

Operation plans for actions, including but not limited to, search/arrest warrant executions, undercover or confidential informant narcotics purchases, or decoy operations should be filed when practicable through the appropriate chain of command unless articulable, extenuating circumstances dictate otherwise. Supervisory notification of said activities shall be made in advance, or as soon as practicable, of said activities in situations prohibitive of filing a formal operations plan.

Surveillance operations involving multiple agencies or law enforcement members beyond the Department should be filed through the appropriate chain of command.

Investigating members are strongly encouraged to document their observations during the course of an investigation. All relevant facts and information shall be included in the investigative report.

All documented observations shall be preserved by the individual member and shall be made available upon request of a supervisor.

Vice/Narcotics/ Organized Crime

Information received related to vice/narcotics/organized crime activities shall be recorded and maintained according to the receiving Station/Section/Unit consistent with other reports of criminal activity. The State Police Detective Unit (SPDU) of jurisdiction shall be notified of criminal activity of this nature that is beyond the scope of the receiving Station/Section/Units investigative capability.

Referral to MSP Station/Section/Units or outside agencies shall be documented in the DAJ or ACISS.

Information received from outside agencies shall be documented and routed to the SPDU of jurisdiction for further investigation as warranted.

The Station/Section/Unit Commander of the investigating unit shall ensure case information of a sensitive or extraordinary nature is provided, as

Vice/Narcotics/ Organized Crime, continued

warranted, and/or available to the Division Commander and/or Colonel/Superintendent.

Designated Rooms for Interviews and Interrogations

- Firearms and Electronic Control Weapons (ECWs) shall not be carried on a member's person during interviews and interrogations, excluding field interviews;
- Care should be taken to ensure that the interview/interrogation room is secured and free of items or hazardous materials that may be utilized to aid the escape of a detainee;
- Equipment necessary to conduct the interview/interrogation should be available in the room prior to initiating the interview/interrogation;
- Audio/video recording of interviews/interrogations shall be in accordance with federal/state statutes and regulations, current case law and Department policy;
- The minimum number of law enforcement personnel will be allowed in the interview/interrogation room and commensurate to the crime committed/investigated;
- Members utilizing said rooms shall have their portable radio on or other means of direct communication with the desk officer or another law enforcement member outside the room;
- Prior to the interview/interrogation, the room should be searched and cleared of any items that could be used as a weapon; and
- The individual being interviewed/interrogated should be provided access to restrooms, water, and/or comfort breaks as circumstances dictate.

References:

Commonwealth v. Glenis A. Adonsoto, 475 Mass. 497 (2016);
Commonwealth v. Hipolito Rosario, 422 Mass. 48 (1996);
Commonwealth v. McNulty, 458 Mass. 305 (2010);
Massachusetts General Laws c.38 s.4;
Massachusetts General Laws c. 66, s 10;
MPAC: 42.1.1, 42.1.4, 42.2.0, 42.2.1, 42.2.2, 42.2.10, 43.1.1, 43.1.4, 55.1.1, 55.1.2, 55.2.1, 55.2.2, 55.2.3, 55.2.4, 55.2.5, 83.2.6.
SP-124: Miranda Rights Warning & Waiver

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**INV-01A**
Subject:	
Case Management	

Policy

Case management is an ongoing process involving all members of the Department. Proper case management facilitates the scope and direction of an investigation, in addition to providing documentation for the Department and court proceedings.

Station/Section/Unit Commanders shall screen cases for investigation to include, but not be limited to:

- Screening of preliminary information received to determine the need for a follow-up investigation;
- Solvability factors related to individual cases to determine the continuation or suspension/termination of investigative efforts; and
- Assignment of personnel and resources to each individual case.

Complaint/ Information

All criminal information, including but not limited to, information relating to vice, drugs, and organized crime that is reported to the Department shall be evaluated for appropriate action. Minimum information required from the original source should include:

- Name;
- Address;
- Telephone number(s);
- Date of birth; and
- Nature of the complaint.

Routine handling of this information shall be relayed to the State Police Detective Unit (SPDU) of jurisdiction, a specialized unit within the State Police, or the local police department of jurisdiction.

Case Management

Case management is an ongoing process involving all members, and is used to maintain records in each case file including, but not limited to, preliminary investigative reports, records of statements, records of arrests, the results of examinations of physical evidence, and case status.

Minimum Complaint Information

For the Division of Field Services (DFS), every case assigned or initiated shall be entered into the Daily Administrative Journal (DAJ) to be maintained by all Stations/Sections/Units. Minimum complaint information to be generated and/or entered shall include:

- Incident number;
- Date of entry;
- Investigating member;
- Complainant's name and address;
- Nature of complaint; and
- If applicable, date and Department section/unit to which the investigative report was forwarded.

For the Division of Investigative Services (DIS) and the Division of Homeland Security and Preparedness (DHS) every case assigned or initiated shall be entered into ACISS Case Management. Barracks utilizing ACISS Case Management shall follow the minimum complaint information requirements of DIS/DHS. Minimum complaint information to be entered shall include:

- Date Initiated;
- Case Officer;
- Case Type;
- Case Description
- Case Status (open/closed/pending/suspended etc.); and
- Case Synopsis within the Case Initiation Report.

Case Number

For DFS barracks utilizing RAMS, all case numbers shall be generated by RAMS.

For Stations/Section/Units utilizing ACISS, all case numbers shall be generated by ACISS.

Case Responsibility

Assignment of a case shall be to a single member who shall:

- Be responsible for the reports on the case;
- Account for evidence; and
- Coordinate the investigative activity and information.

This does not preclude the assignment of additional personnel, nor does it impede the ability of the supervisor(s) to direct investigative efforts or reporting.

Case File

Department Stations/Section/Units shall maintain a case file system utilizing the case number as the primary filing method.

The accessibility to ACISS case files is based on the value assigned to the Case Dissemination field. The accessibility of RAMS case files is all users.

Records and reports relating to active vice, drug, and organized crime investigations shall be securely filed within ACISS case management, separate from the Department's central records system.

Case Dissemination

Within ACISS, Case Dissemination is the method for distributing case information after it has been created. Such dissemination will affect the security of the case. The main classifications of Case Dissemination are:

- **System Wide**: the record is visible to any operator in ACISS Web, regardless of their assignment or the record's assignment;
- **Chain of Command**: the record will be secured according to assignment within the security model. The only operators who can view the case are the Case Lead law enforcement officer, operators listed in the Additional Authorized Users screen, and anyone who has the appropriate security clearance for the case; and
- **Hidden**: the record will be treated as a hidden entity and follow existing access rules for hidden entities. Hiding a case also hides the reports within the case but does not hide Core Entities related to the case.

Case File Retention/ Purging Procedures

All case reports/records/files generated within or uploaded to ACISS or RAMS will be perpetually maintained electronically unless a court order directs the purging of particular case files.

Purging of any other records or case files shall be in compliance with the Secretary of the Commonwealth's retention schedule. Questions on file retention and purging shall be directed to the Department's Legal Section.

Hard copies of case files shall be maintained in secure areas with access limited to authorized personnel. Each MSP facility Officer-in-Charge shall be responsible for the secure storage of hard copies located therein. The central records facility of Department General Headquarters shall be secured and accessible only to authorized personnel. After-hours access shall be authorized and facilitated by the OIC of each facility and limited to members with the lawful authority to access said record(s).

Case File Retention/ Purging Procedures, continued

Release of and/or access to records shall be limited to Department members with an identified investigatory reason for accessing said record(s). Access outside of this limitation shall only be for a lawful reason with the approval of the Station/Section/Unit OIC.

Release of records to requesting law enforcement agencies shall be at the discretion of the OIC of the Department's facility of jurisdiction.

Release of records to the public shall only be made through a formal public records request to be filed with the Massachusetts State Police Legal Section / Public Records Unit. Exceptions to this requirement are provided in SUP-03 Media Relations.

Review/ Approval Process

Reports shall be:

- Reviewed by the reporting member for completeness and accuracy prior to submission;
- Reviewed by a supervisor after submission for completeness and accuracy prior to approval; and
- Returned to the investigating member for further investigation if necessary.

Case Suspension

Station/Section/Unit Commanders shall:

- Approve a request to suspend a case by recommendation of the case member when:
  - Every reasonable avenue of investigation has been pursued and exhausted;
  - There is a lack of further leads or solvability factors;
  - Investigative resources are unavailable due to current workload; and/or
  - The seriousness of the crime is insufficient to justify continued investigative efforts.
- Ensure that the suspension does not preclude the case from being reopened for any reason.

Note: Certain cases due to their serious nature are not eligible for suspended status (e.g., murder, rape, armed robbery).

Subject:	Number:
Case Management	**INV-01A**

Case Termination

Only the Station/Section/Unit Commander shall approve requests to close a case and should consider, at a minimum, the following criteria in determining if a case merits termination:

- Seriousness of criminal offense;
- Availability of investigative resources;
- Unfounded complaint;
- Complainant's refusal to cooperate;
- Referral to another agency;
- Declination by prosecutor;
- Adjudication completed; and
- Administrative closing.

References

SUP-03 Media Relations;
MPAC: 42.1.2, 42.1.3, 43.1.2, 82.1.1, 82.1.3, 82.2.3.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**INV-02**
Subject:	
Confidential Informants	

Policy

The Department shall develop and use confidential informants, as well as other sources of information, as a means to detect, investigate, and prosecute violators of state and federal law.

Definition

Confidential Informant (CI): A person who provides specific information to a Department investigator, and wishes to keep his/her identity confidential.

This does not include "concerned citizens" who provide information on an informal or casual basis.

Special Circumstances

Certain persons should not be used as informants, except in special circumstances with the approval of the Unit Commander. Such persons include:

- Juveniles (a child who has not yet attained their eighteenth (18) birthday), without parental, guardian or legal custodian's approval;
- Persons wanted on warrants;
- Persons with a criminal record for perjury; or
- Persons with a history of serious mental disorder or defect.

Precautions shall be taken to protect the reputations and safety of CIs and investigators. Some CIs may require additional precautions:

- Addicts- should be carefully supervised and controlled;
- Parolees- should be avoided whenever possible. Parolees are prohibited from associating with felons and approval from the CI's parole officer is required.

Note: When meeting with CIs of an opposite sex or sexual preference, members shall ensure that at least two (2) members are present.

Registration of Informants

When a person indicates a willingness to cooperate and provide information, the Unit Commander or designee shall:

- Interview the person as soon as practicable;
- Investigate the background and suitability of the potential CI; and
- Forward the name and biographical data to the appropriate Detective Captain or Major for entry into the Confidential Informant Database.

The Detective Captain/Major shall:

- Check the CI's name against the Undesirable Informant List; and
- Notify the Unit Commander if the CI is currently cooperating and/or assigned to another section/unit.

The recruiting investigator shall:

- Prepare an SP 405 Informant Information Report when the person is approved to be a CI;
- Keep a copy of the SP 405 within the Unit; and
- Debrief the CI regarding their knowledge of other crimes.

Protecting Informant's Identity

The law recognizes the government's privilege not to reveal the identity of a CI. Protecting the identity of all CIs from disclosure is an important factor for two reasons:

1. The CI's safety from retaliation on the part of the criminals they helped implicate; and
2. Disclosure of their identity would prevent the CI from assisting on future investigations.

However, the privilege is not absolute, and should be respected as far as reasonably possible consistent with fairness to a defendant.

Informant Management

Units using CIs shall maintain a file for each CI, in a locked and secure location accessible only to the Unit Commander or designee. This file shall include:

- Code Name and Code Number designations;
- Biographical and background information;
- Criminal history records;
- SP 404 Standard Agreement Statement; and
- Other information deemed necessary by the Unit Commander.

Unit Commanders shall:

- Periodically review and evaluate all CIs' work performance, usefulness, reliability, desirability and records of payment;

Informant Management, continued

- Meet on a semi-annual basis with all registered informants, both confidential and named, and their controlling officers;
- Submit a determination of the status of the informant in writing to the Division of Investigative Services (DIS) Commander or Division of Homeland Security and Preparedness (DHS) Commander by January 15th and June 15th of every year; and
- Upon the termination of an informant, submit in writing to the DIS Commander or DHS Commander the reason for such termination.

Expenditures

Unit Commanders shall ensure expenditures related to a CI be recorded:

- On a SP 406 Confidential Expenditure Fund Voucher; and
- On a SP 407 Confidential Expenditure Fund Log as outlined in INV-02A Confidential Funds.

Unit Commanders shall:

- Not be required to maintain a SP 407 Confidential Expenditure Fund Log when assigned to the Office of the Attorney General, a District Attorneys Office, or a federal task force where there is an internal mechanism for tracking such Confidential Funds.

Undesirable Informants

The primary handler shall submit a report detailing the CI's undesirable conduct to their Unit Commander whenever a CI:

- Endangers officer safety;
- Deliberately gives false or misleading information; or
- Is otherwise determined to be undesirable for use as a CI.

The Unit Commander shall submit to the appropriate Detective Captain/Major:

- Documentation when a CI is terminated for being undesirable;
- A copy of the applicable SP 405; and
- A copy of the primary handler's report.

The Detective Captain/Major shall:

- Place the CI on the Undesirable Informant List maintained by DIS and DHS.

Promises to Informants

Members may:

- Inform the District Attorney or other agencies of the information provided by the CI and the investigation results;

Promises to Informants, continued

- Make recommendations to a District Attorney's Office, probation officer, or other criminal justice agency for a disposition on behalf of the CI; and
- Not make any promises to a CI concerning the outcome of a pending court case.

Note: The disposition of court cases is in the province of the District Attorney's Office and the Judiciary.

Precautions

Interactions and conversations with CIs should be kept to the minimum necessary for effective investigation purposes. Whenever possible and practical, meetings with CIs shall be:

- Attended by two (2) members; and
- With prior notification of the Unit Commander or a supervisor, or as soon as practicable after the meet.

A member who interacts with a known CI, when not on duty or not during the course of an investigation shall:

- Notify their supervisor as soon as practicable; and
- Document the reason for such interaction in the CI's file with a written report.

Whenever practicable, a CI should not report to the Unit's office in order to protect their identity and the identity of other undercover members. CIs shall not:

- Be introduced to more than a minimum number of undercover members, to ensure that CIs gain as little information as possible concerning undercover operations and unit activity.

Any member who uncovers information that a CI has engaged in unauthorized criminal activity shall immediately notify their Unit Commander or designee.

The Unit Commander or designee shall:

- Conduct an immediate evaluation of the information and take such action as they deem necessary; and
- Make every effort to prosecute the CI involved in any unauthorized criminal activity.

Search Warrants

Search warrant applications and their accompanying affidavits containing information from a CI shall be reviewed and approved by a supervisor before filing the application with the court of jurisdiction.

Subject: Confidential Informants	Number: INV-02

Division of Field Services

Members assigned to Field Services who are seeking to use an individual as a CI shall advise their Station Commander.

The Station Commander shall:

- Contact their Division Commander through channels for authorization to manage and register the CI; or
- Contact the appropriate DIS Unit Commander or DHS Unit Commander.

References

INV-2A Confidential Funds;
INV-05 Juvenile Operations;
SP 404 Standard Informant Agreement Statement;
SP 405 Informant Information Report;
SP 406 Confidential Expenditure Fund Voucher;
SP 407 Confidential Expenditure Fund Log;
Commonwealth v. Douzanis 384 Mass. 434,441 (1981);
Commonwealth v. Nelson, 26 Mass. App. Ct. 794 (1989);
Commonwealth v. Lewin 405 Mass. 566 (1989);
Commonwealth v. Brezinski, 405 Mass. 401 (1990);
MGL c.268, §32.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**INV-02A**
Subject:	
Confidential Funds	

Policy

Confidential funds may be used to further investigations, and shall be carefully monitored and supervised.

Expenditure of Confidential Funds

Confidential funds may be derived from the funding mechanisms of the Department, the Office of the Attorney General, and the respective District Attorneys' Offices. Grant monies, forfeiture funds, and funds from state and federal government agencies can be used as payment, if such use is not prohibited by state or federal law.

A Unit Commander may maintain a Confidential Expenditure Fund Account. Access to this account shall be restricted to the Unit Commander and/or supervisors.

The Unit Commander may expend monies from a Confidential Expenditure Fund Account for the following investigative purposes:

- The procurement of evidence;
- Payment to a registered confidential informant for information related to a current documented investigation actively being conducted by the Department;
- Investigative expenses; and,
- The purchase of consumable supplies and other equipment in furtherance of an investigation.

Members shall record expenditures from confidential fund accounts on a SP 406 Confidential Expenditure Fund Voucher and shall include the following information:

- Date of expenditure;
- Amount expended; and
- Supervisor's signature.

Members shall ensure the following information is also recorded on the SP 406 where applicable:

- Signature of the member, a witnessing member and the CI confirming receipt of funds.

Note: CI may use real or assumed name when signing receipt.

Subject: Confidential Funds	Number: INV-02A

Expenditure of Confidential Funds, continued

Unit Commanders shall maintain a SP 407 Confidential Expenditure Fund Log reflecting:

- The transaction number (expenditures only, from the SP 406);
- The amount of expenditure or deposit; and
- The balance of the account.

Accounting and Audits

Prior to the transfer of a Unit Commander, there shall be reconciliation of the accounting records and of the monies on hand with the incoming Unit Commander.

Each quarter, Unit Commanders shall review, evaluate, and analyze all records of expenditures to ensure funds are being used in a cost-effective manner.

An internal audit of all accounting records and accounting practices shall be conducted annually by the appropriate Division Commander.

An audit of Confidential Funds files may be conducted as directed by the appropriate Division Commander or as directed by the Colonel/ Superintendent.

Exceptions

Unit Commanders shall not be required to maintain a SP 407 Confidential Expenditure Fund Log under the following conditions:

- Members who are assigned to the Office of the Attorney General, a District Attorneys' Office, or a federal task force; and
- An internal mechanism exists for tracking Confidential Funds.

References: SP 406 Confidential Expenditure Fund Voucher;
SP 407 Confidential Expenditure Fund Log;
MPAC: 42.2.7.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**INV-03**
Subject:	
Prescription Monitoring Program	

Policy

Only members designated by the Department may access or use information contained within the Prescription Monitoring Program. Access to the system must be pursuant to a bona fide, specific controlled substance investigation or a related criminal investigation.

Any member, who violates this policy and/or state regulations related to the Prescription Monitoring Program may face disciplinary action, as well as loss of access to the Prescription Monitoring Program.

Purpose

The purpose of the Prescription Monitoring Program is to assist health care providers and investigative agencies in addressing drug diversion and the misuse and abuse of pharmaceutical controlled substances.

The Prescription Monitoring Program is a computer-based system that collects prescription data submitted by pharmacies on most prescriptions for controlled substances in Schedules II through V.

Massachusetts General Laws (MGL) c. 94C §24A established the Prescription Monitoring Program within the Department of Public Health (DPH) effective January 1, 2011. The DPH shall, upon request, provide data from the Prescription Monitoring Program to local, state and federal law enforcement or prosecutorial officials working with the Executive Office of Public Safety and Security engaged in the administration, investigation or enforcement of the laws governing prescription drugs; provided, however, that the data request is in connection with a bona fide, specific controlled substance or additional drug-related investigation.

Access to the Prescription Monitoring Program

The Department shall:

- Authorize sworn members assigned to the Division of Investigative Services (DIS) and the Division of Homeland Security and Preparedness (DHS) to access and use information obtained via the Prescription Monitoring Program in accordance with state regulations.

According to state regulations, any member granted access to the Prescription Monitoring Program shall:

- Successfully complete any and all required training; and
- Not share their passwords or codes with any other person.

Subject:	Number:
Prescription Monitoring Program	**INV-03**

Use of Data From the Prescription Monitoring Program

Data ascertained from the Prescription Monitoring Program:

- May only be used in furtherance of the official Department investigation for which it was requested;
- May only be shared with authorized personnel from other law enforcement agencies or with state and federal prosecutors who are working on the matter for which it was requested; and
- Shall not be disseminated to others.

Designated members are:

- Allowed to use the Prescription Monitoring Program and the associated data only in connection with the bona fide specific controlled substance related criminal investigation for which it was requested.

Members shall not use the data or information from the Prescription Monitoring Program:

- For the furtherance of any illegal act, including violation of any criminal or civil laws or regulations;
- For any political or commercial purpose;
- To libel or otherwise defame any person(s); or
- For any matter other than the one for which it was requested.

Prior to accessing the Prescription Monitoring Program, the member shall:

- Notify their supervisor;
- Open an investigation;
- Obtain a Department Case Number; and
- Write a short narrative that includes information leading to the belief that prescription drugs are being diverted for illegal purposes.

Supervisor Responsibilities

Responsibilities of DIS and DHS Supervisors shall include:

- Ensuring that members under their command comply with the provisions of this policy and MGL c.94C §24A;
- Monitoring members' use in order to ensure compliance; and
- Notifying the Prescription Monitoring Program Administrator when a designated member transfers from the unit.

References MGL c. 94C §24A.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**INV-05**
Subject:	
Special Protections for Juveniles	

Policy

Courts recognize the vulnerability of children. The Department shall ensure that juveniles are afforded special protections during interrogations.

Definitions

Interested Adult: An adult in a position, where he or she is an advocate or has the best interest at heart for the juvenile. The adult shall be eighteen (18) years of age or older and preferably be a parent or legal guardian, or an adult sibling, relative, friend, or attorney.

Juvenile: A child who has not yet attained his or her eighteenth (18) birthday.

Juveniles and Miranda

The duration of questioning and the number of members present should be as minimal as possible both to prevent a coercive atmosphere and to protect the juvenile's rights.

Before proceeding with a custodial interrogation of a juvenile, Miranda Warnings shall be given in accordance with the following table, and in the presence of the juvenile, their parent, guardian, or other interested adult.

The juvenile shall then be allowed to have a meaningful consultation with the adult. Written waivers are preferred.

If the Juvenile's Age is…	Then…
Under twelve (12) years of age.	No criminal charges can be filed. They shall not be questioned, unless a parent or interested adult is present.

Juveniles and Miranda, continued

If the Juvenile's Age is…	Then…
Twelve (12) years of age and not yet attained his or her fourteenth (14) birthday.	Criminal charges can be filed. The juvenile shall not be questioned, unless a parent or interested adult is present. The interested adult and the juvenile must have an actual opportunity to discuss their rights in private. Moreover, police *must* honor any request by the juvenile or adult to meet privately. Questioning can only commence when the juvenile and the adult indicate that they understand the rights and the consequences of waiving these rights; and when the juvenile expressly waives his or her rights.
Fourteen (14) years of age, but not yet attained his or her eighteenth (18) birthday; and a parent or interested adult is not available after reasonable efforts are made to contact them.	Criminal charges can be filed. The juvenile must be given the opportunity to have a meaningful consultation with an interested adult before he or she can waive Miranda rights. The best practice dictates that the interested adult and the juvenile be given the opportunity to confer in private. Moreover, police *must* honor any request by the juvenile or adult to meet privately. However, a statement *may* be taken if the juvenile demonstrates a high degree of intelligence, experience, knowledge, or sophistication in understanding the Miranda warnings and the consequences of waiving his or her rights and expressly waives his or her rights.

Subject: Special Protections for Juveniles	Number: INV-05

Special Considerations

Members may have to take extra steps to ensure that juveniles understand their rights. This may include explaining or repeating the Miranda rights, or explaining Department procedures or juvenile court procedures to the juvenile.

Other factors to consider are the juvenile's level of schooling, maturity, history of interaction with the juvenile justice system, and any mental or emotional conditions.

References

MGL c.111B § 8;
MGL c.119, § 1, § 21, § 34, § 39, § 39H, § 66, § 67, § 68B;
MGL c.138, § 34C;
MGL c.276, § 5758;
MGL Session Law-Acts of 2012 c.240;
MGL Session Law-Acts of 2013 c.3 § 5B;
Juvenile Justice & Delinquency Prevention Act of 1974 and 2002 (42 USC 5601).

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**INV-07**
Subject:	
Non-Published Telephone Numbers	

Policy

Telephone company records shall only be obtained when necessary for the furtherance of a criminal investigation or in an emergency.

Statutes

Administrative Subpoena: Issued in the form of a demand letter for telephone company records and may only be authorized by the Attorney General or District Attorney of jurisdiction. Massachusetts General Laws (MGL) c.271, §17B.

Electronics Communications Privacy Act: Limits access to certain records maintained and stored by a common carrier such as a telephone company. The act sets forth the requirements needed to obtain such records. (18 USC, §2703)

Authority For Obtaining Records

In order to obtain telephone records, authority may only be granted by:

- Administrative subpoena authorized by the Office of the Attorney General or District Attorney of jurisdiction;
- State or federal grand jury or trial subpoena;
- State or federal warrant;
- State or federal court order; or
- Consent of the customer or subscriber to such disclosure.

Records Available

When a member has reasonable suspicion to believe that the service of a common carrier is being or may be used for an unlawful purpose, they may request, through the Office of the Attorney General or the District Attorney's Office of jurisdiction an administrative subpoena for release of records from the common carrier to include, but is not limited to:

- Listing of a non-published telephone number;
- Listing of all optional services;
- Telephone toll records and optional services;
- Telephone services, including non-published numbers; and
- A copy of the contract, listing, and monthly bills for a cellular phone and electronic paging.

Subject:	Number:
Non-Published Telephone Numbers	**INV-07**

Procedure

Members shall submit a request through proper channels to the Attorney General or District Attorney requesting a subpoena for the required information.

The request shall:

- Detail the grounds for the member's belief that the telephone is being used for an unlawful purpose; and
- Include the case number and the signature of the member's Commanding Officer.

Members shall also follow any written directives promulgated by the Office of the Attorney General or the District Attorney's Office of jurisdiction to request telephone records.

Members not assigned to the Office of the Attorney General or a District Attorney's Office shall contact, through proper channels, the appropriate State Police Detective Unit (SPDU) Commanding Officer for assistance in determining the policy of the respective jurisdiction.

Emergencies

Troop Duty Officers or Unit Commanders may authorize members to contact the Directory Assistance Operator in emergency situations, such as a serious motor vehicle accident or threat of imminent harm. The member shall:

- Request the operator contact the non-published customer; and
- Inform the customer to call back the member.

This alternative shall not be used to facilitate investigative inquiries, such as attempting to locate a witness.

Reports

Non-published numbers obtained pursuant to a criminal investigation shall be properly documented in the record of investigation in order to:

- Provide the information to the Criminal Information and Intelligence Section; and
- Eliminate duplicate requests to the common carrier, when possible.

When a non-published number is included in a report it shall be clearly noted as such, so that it is not released to the public via the record of investigation.

References: MGL c.271, §17B;
18 USC, §2703.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**INV-08**
Subject:	
Criminal Intelligence	

Policy

The Department shall share criminal intelligence among the criminal justice community in an effort to prevent and control crime while protecting the privacy and constitutional rights of individuals.

Definitions

Content Validity: Refers to the accuracy or truth of the information.

Criminal Information: Raw data, gathered by law enforcement agencies in the normal course of performing their duties, which is maintained as directed by statute or policy.

Criminal Intelligence Information: Information that has been evaluated and determined to be of value to criminal investigations.

Criminal Intelligence System: The equipment, facilities, and procedures used for the receipt, storage, exchange, dissemination, and analysis of criminal intelligence information.

Need-to-Know: The necessity to obtain or receive criminal intelligence information in the performance of official responsibilities as a law enforcement authority.

Reasonable Suspicion: When information exists that provides sufficient facts to believe that there is a reasonable possibility an individual or organization is involved in a definable criminal activity or enterprise.

Right-to-Know: The legal authority to obtain or receive criminal intelligence information pursuant to a court order, statute, or case law.

Source Reliability: Refers to the reliability of the source of the information.

Security

Criminal intelligence information shall be stored in a criminal intelligence database that prevents unauthorized access.

The criminal intelligence database shall provide an audit trail that tracks:

- What intelligence was accessed;
- Who accessed the intelligence; and
- The date and time when the intelligence was accessed.

Collection

Criminal intelligence information shall only be collected and maintained if there is reasonable suspicion to believe that an individual, group or organization is involved in criminal activity and the information is relevant to criminal conduct or activity.

Electronic surveillance shall only be conducted in accordance with all applicable state and federal regulations.

Photographic surveillance shall only be conducted in an effort to identify individuals or groups who are believed:

- To have participated in criminal activity;
- To be planning criminal activity; or
- Are currently engaged in criminal activity.

Each criminal intelligence submission shall be attributable to a credible source. All criminal intelligence information shall be forwarded to the Criminal Information and Intelligence Section (CIIS), as soon as possible, using one of the following methods:

- Direct Entry: Information entered by an authorized member into the criminal intelligence database directly from an authorized Department computer; and
- Indirect Entry: Information entered by CIIS on behalf of a member who does not have authorized access to the criminal intelligence database.

Note: CIIS may be contacted for guidance, clarification, and additional support to facilitate criminal intelligence submissions.

Collection, continued

Members who submit information for entry into the criminal intelligence database shall classify the source(s) as:

- Completely Reliable: The source is unquestioned or has been tested successfully in the past; or
- Usually Reliable: The source can usually be relied upon. The majority of information provided in the past has proved to be reliable; or
- Unreliable: The source has been determined to be unreliable in the past; or
- Reliability Unknown: The source cannot be judged. Its authenticity or trustworthiness has not yet been determined by either experience or investigative corroboration.

Members who submit information for entry into the criminal intelligence database shall classify the validity of the information as:

- Confirmed: Has been corroborated by an investigator or another reliable independent source; or
- Probable: Is consistent with past accounts; or
- Doubtful: Is inconsistent with past accounts; or
- Cannot Be Judged: Validity of the information cannot be judged, or its authenticity has not yet been determined.

Note: A source classified as "Reliability Unknown" combined with a content validity rating of "Cannot Be Judged" would not meet the burden of reasonable suspicion for inclusion into the criminal intelligence database.

Information concerning individuals or organizations not reasonably suspected of criminal activity that is entered into the criminal intelligence database, shall be marked as "non-criminal identifying information."

Restrictions

Information and criminal intelligence shall not be collected or developed solely on the basis of an individual or group's:

- Support of a particular cause;
- Race;
- Color;
- Religion;
- Gender;
- National origin or ancestry; or
- Political affiliation.

Information pertaining to the above listed factors shall only be collected and maintained if the information directly relates to criminal conduct, and there is reasonable suspicion that the subject is or may be involved in criminal activity.

Subject: Criminal Intelligence	Number: INV-08

Dissemination

Submitting Department entities are responsible for the review and evaluation of data entered into the criminal intelligence database and establishing dissemination levels. Criminal intelligence information shall only be disseminated:

- In the furtherance of an authorized law enforcement activity;
- To authorized law enforcement or criminal justice personnel; and
- On a "need-to-know" and "right-to-know" basis.

Review/Purge

Intelligence information held within the criminal intelligence database shall be:

- Reviewed on a continual basis;
- Purged when found to be obsolete or inaccurate; and
- Purged when information has not been updated or verified for five (5) years from date of entry.

The Commanding Officer of CIIS, when determining whether or not to purge intelligence records contained within the criminal intelligence database shall:

- When feasible, contact the member or agency which contributed the intelligence information to determine if any additional intelligence may be added to update the record;
- Purge the record from the system if there is no additional intelligence;
- Ensure only an administrative record of the purge is maintained; and
- Ensure there is no record of the original criminal intelligence information maintained within the system.

References: MGL c.22C, §38;
MGL c.272, §99;
28 CFR Part 23;
MPAC: 46.3.2.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**INV-09**

Subject:

Polygraph Examinations

Policy

The Department shall use the polygraph with great selectivity, and then, only as an investigative tool.

Polygraph Examiners

Department Polygraph Examiners shall be designated by the Colonel/ Superintendent.

Polygraph Examiners must be graduates of institutions providing certified training for this purpose.

Restrictions on Polygraphs

In general, an employer cannot require, request or suggest that an employee or job applicant take a polygraph within or outside the Commonwealth. (Massachusetts General Laws (MGL c.149, §19B).

Polygraph examinations may not be used for any person applying for employment. Department recruit applications shall contain the following notice:

"It is unlawful in Massachusetts to require or administer a lie detector test as a condition of employment or continued employment." (MGL c.149, §19B(2)(b).)

At present, polygraph evidence is inadmissible in criminal trials and may not be used in a criminal trial for any purpose. (Commonwealth v. Mendes, 406 Mass.201, 212 (1989)).

Subject:	Number:
Polygraph Examinations	**INV-09**

Administering an Examination

Under MGL c. 149, §19B law enforcement agencies are permitted to administer a polygraph examination when the polygraph is requested as part of a criminal investigation.

Submission to the polygraph examination must be a voluntary act on the part of the examinee, and the voluntary nature of the exam does not invalidate the constitutional rights of the examinee.

Prior to an examination, the examinee shall sign:

- A statement of voluntariness; and
- A witnessed waiver of any rights against the Polygraph Examiner and the Department.

Polygraph Examiners should include a copy of their certificate/qualifications in each case file, and if technical tools are used, they should be used in accordance with the examiners training.

Requesting an Examination

To request an examination, Department members shall contact the Polygraph Unit through appropriate channels.

Any requests from local, state or federal agencies shall be referred to the Polygraph Unit. The Polygraph Unit may decline to conduct an examination.

It is the responsibility of the requesting agency to provide the background of the case and transportation of the examinee to and from the place of examination.

Preparing for an Examination

The member requesting the examination is responsible for providing the Polygraph Examiner with pertinent information concerning the case including:

- Information that supports and justifies the use of the polygraph;
- Investigative reports;
- Evidence available and withheld from the subject;
- Background information on the subject;
- Statements made by the subject, complainants, and witnesses including alibis; and/or
- Newspaper articles or other general information concerning the case.

Members shall not:

- Interrogate a subject immediately before they are to take a polygraph; or
- Attempt to explain procedures that shall be used in the examination.

Subject:	Number:
Polygraph Examinations	**INV-09**

Internal Investigations

No member of the Department shall be subjected to a polygraph examination for a violation of written directives, except in cases of alleged criminal conduct.

Department Polygraph Examiners shall not be required to conduct examinations on members of the Department.

The Commander of the Polygraph Unit shall establish reciprocal agreements with other State Police agencies for examinations, when warranted, and as approved by the Colonel/Superintendent.

Department members may assist other state and local law enforcement agencies with internal investigations that involve allegations of criminal wrongdoing. Requests for examinations shall:

- Be in writing; and
- Contain a statement that the polygraph is for a criminal investigation.

References

MGL c.149, §19B;
Furtado v. Plymouth 69 Mass. App. Ct. 319 (2007), and SJC-10049 (2008);
Baglioni v. Chief of Police Of Salem, 421 Mass. 229 (1995);
Commonwealth v. Mendes, 406 Mass.201, 212 (1989);
Patch v. Mayor of Revere, 397 Mass. 454 (1986);
Baker v. Lawrence, 379 Mass. 322 (1979);
International Brotherhood of Police Officers v. Labor Relations Commission 391 Mass. 429 (1984);
Carney v. the City of Springfield 403 Mass. 604 (1988);
MPAC: 42.2.6.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**INV-10**
Subject:	
Evidence Collection and Preservation	

Policy

The Department shall ensure that evidence is properly recognized, documented, collected, packaged, and stored; and shall ensure that a documented chain of custody is established for evidence recovered at every crime scene. Training shall be required for employees in the proper collection methods of evidence related to their assignment.

All evidence that comes into the possession of a member shall be entered into the evidence control function prior to the end of the member's shift unless exigent-documented circumstances prevent the return, or entering, of said evidence. In the event of an exigent-documented circumstance, the evidence shall be entered in at the next most practicable time. Such delay and the steps taken to safeguard the evidence in the intervening time shall be documented in the incident/investigative report. A descriptive inventory of the evidence shall be made verbally to the Troop Duty Officer, who shall then document it in the Daily Administrative Journal (DAJ). The Troop Duty Officer shall be the approving authority for any documented delay.

Definitions

Chain of Custody: The record documenting the location and person in control of evidence from the time of its collection to final disposition.

Evidence Room: Facilities used by the Department to store and preserve evidence.

Crime Lab Services

The Massachusetts State Police Crime Laboratory (MSPCL) provides forensic services to the Commonwealth. Members of the MSPCL are divided into several different units or sections and are trained and equipped to recognize, document, collect, preserve, and process many types of evidence and are available 24/7 to provide required services.

Crime Scene Response Unit (CSRU) is a unit comprised of forensic scientists available to respond to crime scenes. Services rendered shall be documented. Services include, but are not limited to:

- Documentation, collection and preservation of biological (DNA) evidence including blood, semen, and saliva;
- Documentation, collection and preservation of gunshot residue and trace evidence such as hairs, fibers, and paint; and
- Documentation, collection, preservation, and analysis of bloodstain patterns.

Crime Scene Services Section (CSSS) assists with the recognition, collection, processing, preservation, and documentation of many types of physical evidence. Services rendered shall be documented. Services include, but are not limited to:

- Documentation of crime scenes through photographs, videos, diagrams, and sketches;
- Collection and processing of footwear, tire track impression evidence, and latent print evidence; and
- Collection and preservation of other types of physical evidence.

Firearms Identification Section (FIS) is available to respond to crime scenes: Services rendered shall be documented. Services include, but are not limited to:

- Documentation, collection, and preservation of firearms and related evidence.

Other Services

Cyber Crime Unit is assigned to the Division of Homeland Security (DHS) and assists with the recognition, collection, preservation, and examination of computers and other digital evidence devices (e.g., cell phones, cameras, and digital storage media). This unit can provide field assistance by drafting search warrants for digital evidence crime scenes and digital evidence seizures.

Collision Analysis & Reconstruction Section (CARS) assists with the technical analysis of crash scenes. Services include:

- Documentation of crash scenes through diagrams and sketches;
- Documentation, collection, and preservation of crash-related evidence, including vehicle components such as airbags, lamps, tires, and bumpers;
- Vehicle inspections, including the documentation, collection, and preservation of Airbag Control Modules (ACM), Powertrain Control Modules (PCM), and vehicle media systems; and
- Forensic mapping and diagramming of crime scenes through the use of Unmanned Aircraft Systems (UAS).

Arriving at a Crime Scene

Evidence of a criminal nature may be encountered at any incident or call. When arriving at a scene, members should consider the nature of the incident or crime, the jurisdiction, and their investigative authority in the context of recovering evidence of a crime.

Subject: Evidence Collection and Preservation	Number: INV-10

Arriving at a Crime Scene, continued

Members arriving at a scene shall:

- Attempt to identify and control any dangerous situations or persons while bearing in mind the safety of the public and the officer;
- Ensure that medical attention is provided to injured parties;
- Take care when removing the injured or rendering the scene safe and secure; and
- Be mindful that any action taken may affect or alter a potential crime scene and should be documented; and
- Establish boundaries beyond the initial scope of the crime scene perimeter with the understanding that boundaries can be reduced, but cannot be easily expanded.

Crime Scene Evaluation

When a scene requires specialized investigative and forensic units, responding members shall:

- Secure the scene and treat the area as a crime scene;
- Evaluate the nature of the event or crime and the resources required to effectively respond to the situation; and
- Preserve the scene with the goal of preventing contamination and disturbance of potential evidence.

Members shall:

- Notify the Desk Officer or appropriate supervisor of all actual or potential crime scenes;
- Request assistance through the Desk Officer from other patrols, supervisor(s), investigative, or forensic units as necessary;
- Document and relay to appropriate supervisory, investigative, or specialized personnel relevant activities and observations made; and
- Document in an investigative report all information related to the crime scene including the notification of specialized units.

Desk Officers shall:

- Notify the Troop Duty Officer of complex crime scenes that require specialized assistance.

Troop Duty Officers shall:

- Request the assistance of specialized units when the scene requires skills or equipment beyond those of the initial responding member(s); and
- Document the specialized unit(s) notifications in the DAJ/ACISS.

Crime Scene Command and Control

Responding members shall:

- Remain in charge of the scene until command is transferred to a supervisor or to the responding specialized unit(s);
- Continue to provide assistance until released; and
- Document activities while at the scene and include these in a written report.

Subject: Evidence Collection and Preservation	Number: INV-10

Crime Scene Perimeter and Control

Members responding to a crime scene shall:

- Establish a crime scene perimeter;
- Establish boundaries beyond the initial scope of the crime scene perimeter with the understanding that boundaries can be reduced, but cannot be easily expanded;
- Control access to the scene to authorized personnel only; and
- Document the names of all persons who accessed the scene.

Recovery of Evidence

Crime scenes shall be documented prior to processing and searching. Documentation may include:

- Written description;
- Photographs and videos;
- Sketches and diagrams; and
- Three-Dimensional High Definition Surveying.

Members may collect any evidence that does not require assistance from specialized units. Members shall take steps to minimize the handling of evidence. Members shall:

- Wear gloves during evidence collection;
- Understand that when gloved, the handling of evidence may destroy or damage latent fingerprint and DNA evidence; and
- Package evidence in a manner to preserve and prevent spoilage or contamination.

All evidence shall include a detailed description and recovery location. The item labels shall be recorded on the outside of each packaged item and include:

- The case identifier/number;
- Seizing member's name and identification (ID) number;
- The date, location of seizure, and description of the item(s); and
- Initiation or continuation of a documented chain of custody on all evidence.

When multiple items are recovered from a single location, members shall sequentially number items for identification purposes.

When personnel from specialized units collect evidence, they shall adhere to their respective policies and directives.

Recovery of Evidence, continued

Members shall take appropriate precautions when collecting or storing biological matter or chemical substances that may pose serious health risks if handled improperly or unprotected.

- Evidence requiring refrigeration collected outside of the MSPCL operating hours shall be transferred to the locked refrigeration unit located in the Troop HQ of jurisdiction unless otherwise directed by a specialized unit Supervisor. This transfer shall be documented utilizing the appropriate chain of custody forms with notations in the DAJ of both the sending and receiving locations as well as notification to the evidence officer of the sending location;

The MSPCL provides evidentiary guidelines on the proper methods to collect and package different types of evidence. Members may contact the MSPCL for guidance on proper evidence collection and preservation.

Crime Scene Special Circumstances

DNA Evidence

Crime scenes often contain items of evidence that may be amenable to DNA testing.

- MSPCL CSRU should be contacted to assist at scenes when biological screening services are required or when assistance with biological evidence collection is needed.
- Members on scene shall be properly trained in and employ practices to prevent potential contamination of DNA evidence. Such practices include but are not limited to the use of proper Personal Protective Equipment, minimizing personnel within the scene, and collecting and packaging items of evidence using materials appropriate for the preservation and storage of biological material. (Refer to MSPCL Information Papers for proper packaging guidelines).

Photography and Video recording of Crime Scenes

Most crime scenes are documented by MSPCL CSSS. When alternative documentation is needed, the following steps should be followed:

- Take establishing photographs (overall), to depict the location using street signs, addresses, or other geographical information when possible.
- Take overall photographs of the exterior of the crime scene.
- Take overall photographs of the interior of the crime scene.
- Assign unique identifiers to items of evidentiary value when determined appropriate by scene personnel. Take additional photographs that include these markers.
- Take mid-range and close-up photos of items of interest.

Crime Scene Special Circumstances, continued

- Close up photographs for comparative quality photographs should include a scale and be taken with the film plane of the camera parallel to the evidence.
- Any photo or video documentation shall be noted in the scene report.
- Photo or video documentation evidence shall be processed in accordance with established procedures pursuant to policy, section/unit SOP, and applicable statutory/case law.

Fingerprinting of Crime Scenes

In cases where processing for latent prints is required, members shall utilize the services of the CSSS. In many instances, the evidence may be documented, collected, and submitted to the MSPCL for processing according to this policy.

DNA Collection of Known Source

- Materials and substances should be considered for collection from a known source for submission to the MSPCL for comparison with physical evidence collected.
- Collection of known source standards for DNA analysis shall be done in accordance with MSPCL procedures. Officers performing collection shall be trained by MSPCL personnel prior to performing these collections.

Evidence

Station/Section/Unit Commanders shall be responsible for receiving, storing, maintaining, releasing, and accounting of all evidence.

Commanders shall ensure that:

- Evidence is placed into the evidence room or other authorized secure location prior to the end of the member's shift;
- A written report detailing a full accounting of the property/evidence, the circumstances by which the property/evidence came into the agency's possession is completed;
- When analysis is required, evidence is promptly submitted to the appropriate facility;
    - Items with evidentiary value that are too large to be secured in the temporary evidence locker should be photographed to memorialize the original evidentiary state and be stored in an area that is secure and maintains the integrity of the evidence prior to processing.
- Evidence is packaged and labeled according to specific evidentiary requirements consistent with Department policy and MSPCL recommendations;
- Efforts are undertaken to identify and notify the owner or custodian of property in the agency's custody;
- Establish procedures for the temporary and final release of property items from the control of the property and evidence function;

Evidence, continued

- Evidence that comes into the possession of the Department that is of an exceptional, valuable, and/or sensitive nature shall require additional security measures based upon the real and/or recognized value including alternative authorized storage and/or Supervisory notification as necessary; and
- The temporary and final release of evidence shall be guided by court order.

Any member who recovers or receives evidence to be placed in the evidence room shall have evidence documented at the appropriate station using appropriate Department forms and recorded in the DAJ. The inventory shall be witnessed and shall include the following information for all items of evidence:

- Description of the item (including make, model number, and serial number, if any);
- Source (from whom or location obtained); and
- Name of person primarily responsible for collecting the item or items.

Evidence Lab Submission

For evidence being submitted to the MSPCL, members shall refer to the MSPCL Information Papers listed in the reference section below, accessible via https://www.mass.gov/how-to/submit-evidence-to-the-crime-lab, and contact the MSPCL Evidence Control Unit to schedule an appointment. Evidence shall be hand delivered to the MSPCL.

Submissions of drug evidence shall be accompanied by SP 295 Drug Submission Form.

Submissions of non-drug evidence shall be accompanied by the MSPCL Evidence Submission Form.

A copy of the police report should be provided at the time of submission, if available, or as soon as possible.

Receipts of evidence submission shall be obtained from the MSPCL by the submitting officer.

Subject:	Number:
Evidence Collection and Preservation	**INV-10**

References
INV-11 Controlled Substances – Storage and Handling;
INV-11A Contraband – Storage and Handling;
INV-14 Seized Currency;
SP 295 Drug Submission Form;
MSPCL Evidence Submission Form;
MSPCL ECU Arson & Explosives Unit Information Paper;
MSPCL ECU Packaging Guidelines for Evidence Information Paper;
MSPCL ECU Sexual Assault Evidence Collection Kit Information Paper;
MSPCL ECU Submission of Drug Evidence Information Paper;
MSPCL ECU Trace Hair Information Paper;
MSPCL ECU Trace Paint Information Paper;
MPAC: 83.1.1, 83.2.1, 83.2.2, 83.2.3, 83.2.5, 83.3.1, 83.3.2, 84.1.1.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**INV-11**

Subject:

Controlled Substance Intake-Storage

Policy

The Department shall establish rigid protocols for all controlled substances held within its custody to preserve the integrity of the Department and its personnel.

Controlled substances shall not be stored in vehicles or personal storage areas. Members who come into the possession of controlled substances shall transport said controlled substances directly to their Station/Section/Unit for entry into the Evidence/Contraband/Property (ECP) control function. Exceptions to direct transport shall be guided by this policy.

All ECP that comes into the possession of a member shall be entered into the ECP control function prior to the end of the member's shift unless exigent-documented circumstances prevent the return, or entering, of said ECP. In the event of an exigent-documented circumstance, the ECP shall be entered in at the next most practicable time. Such delay and the steps taken to safeguard the ECP in the intervening time shall be documented in the incident/investigative report. A descriptive inventory of the ECP shall be made verbally to, and documented in the DAJ by the Troop Duty Officer, who shall be the approving authority for any documented delay.

A written report detailing a full accounting of the ECP and the circumstances by which the controlled substance(s) came into the Department's possession shall be completed, including the submission of affiliated evidence/property forms.

Through the assignment of responsibilities, processing procedures, storage requirements and continuous inspections, all levels of command shall ensure strict compliance with established controls and this policy.

Definitions

Chain of Custody: The record documenting the location and person in control of ECP from the time of its collection to final disposition.

Controlled Substances: All narcotics, drugs, and substances listed in Massachusetts General Laws (MGL) Chapter 94C.

Department Evidence Officer: A member appointed by the Colonel/Superintendent as the Narcotics Inspection Unit Commander who shall to act as custodian of all controlled substances seized in the course of any arrest or investigation by the Department.

Definitions, continued

ECP Custodian: Station/Section/Unit Commander responsible for receiving, storing, maintaining, releasing, and accounting of all evidence, contraband, found, unclaimed and abandoned property within their facility.

Narcotics Central Evidence Locker (CEL): A secure location located within the State Police Troop of Jurisdiction. Each CEL is staffed by the Narcotics Inspection Unit personnel. NIU personnel assigned to the CEL shall have direct control and responsibility for the handling, storage, and security of controlled substances seized by members located within their Troop Jurisdiction.

Narcotics Inspection Unit (NIU): The unit shall exercise administrative control and supervision of procedures concerning the marking, recording, storage, handling, disposal, and destruction of all controlled substances obtained or seized by members of the Department.

NIU Bunker: Narcotics Locker located at the State Police General Headquarters used to store controlled substances that have been transported from a Station/Section/Unit or Central Evidence Locker and are awaiting trial, destruction, or disposal.

Temporary Controlled Substance Evidence Locker: Temporary limited access storage area/locker within Department facilities for controlled substances that come into the possession of the Department.

Responsibilities

Position	Responsibilities
Narcotics Inspection Unit Commander	• Assume responsibility and duties specified in MGL c.94C, §47A, as the "Evidence Officer" for the Department; • Shall have command and control of the Narcotics Locker (NIU Bunker) located at General Headquarters; • Maintain oversight and/or access to all Department Temporary Controlled Substance Evidence Lockers.
Troop/Section Commanders	• Ensures the security and safeguarding of all controlled substances held in all Stations/Sections/Units under their command.
Station/Section/Unit Commander	• Has the responsibility as the "ECP Officer" of their Station/Section/Unit; • Has direct control and responsibility for the handling, storage, and security of controlled substances seized by members under their command; • Retains responsibility of all controlled substances and ensures adherence to Department Policy and Procedures; • Ensures that members under their command are trained and familiar with the appropriate handling and storage of controlled substances; and

Responsibilities, continued

	• Notifies the NIU or CEL forthwith to make arrangements for the transportation of the controlled substances according to NIU procedures. In addition, Station/Section/Unit Commander may: • Delegate the duties of the ECP Officer to any member under their command; and • Designate that member to serve as the "Assistant ECP Officer" for that Station/Section/Unit.
Investigating Member of Controlled Substance(s)	Upon arrival at the Station/Section/Unit the Investigating Member shall: • Log the controlled substance(s) into the Station/Section/Unit Daily Administrative Journal and in the Temporary Controlled Substance Evidence Locker Journal; Prior to the end of their shift the Investigating Member shall: • Tag each item or place each item in a Department Evidence bag with the information listed below. o Defendant's name(s); o Defendant's DOB; o Case number; o Date seized; o Location where seized; and o A brief description of the item, listing the quantities on the evidence packaging and chain of custody form. **NOTE:** Controlled substances to be submitted for testing shall be packaged separate from other ECP that *does not* require testing. • Indicate whether the controlled substance(s) have been transferred: o Directly to the ECP Officer, NIU Unit Commander/designee; or o The controlled substance(s) have been placed in the Temporary Controlled Substance Evidence Locker with entries made into the Temporary Controlled Substance Evidence Locker Journal. • Ensure that the SP 295 Drug Submission Form is completed. Note: See Controlled Substance Storage Area within this policy for controlled substances that are too large to fit into the Temporary Controlled Substance Evidence Locker.

Station/Section/ Unit ECP Officer

The Station/Section/Unit Commander or ECP Officer shall:

- Maintain the Temporary Controlled Substance Evidence Locker Journal issued by the Narcotics Inspection Unit;
- Ensure the Temporary Controlled Substance Evidence Locker Journal is kept near the Temporary Controlled Substance Evidence Locker;
- Check the Temporary Controlled Substance Evidence Locker Journal and Temporary Controlled Substance Evidence Locker during their shift for items that may have been deposited;
- Contact NIU and/or the CEL when controlled substances have been seized and are in the Temporary Controlled Substance Evidence Locker; and
- Ensure that the controlled substances are properly labeled and packaged by the Investigating Member and that they have completed the SP 295.

Note: Access to Controlled Substances placed into Division of Field Services Barracks Temporary Controlled Substance Evidence Locker shall be limited to the NIU Commander or designee.

Note: Assistant ECP Officers shall perform duties as directed by the Station/Section/Unit Commander.

Controlled Substance Storage Area

Temporary Storage

Each Station/Section/Unit shall:

- Be provided with a Temporary Controlled Substance Evidence Locker with twenty-four (24) hour access to all authorized personnel;
- Allow for the temporary secure storage of controlled substances; and
- Have available a Temporary Controlled Substance Evidence Locker Journal to enter all pertinent information.

The ECP Officer shall:

- Ensure that the Temporary Controlled Substance Evidence Locker remains securely locked at all times; and
- Prevent access to unauthorized personnel.

Permanent Storage

Permanent Storage of controlled substances shall:

- Be stored at the CEL of jurisdiction and the NIU Bunker with access limited to authorized personnel; and
- Not be stored in vehicles or personal storage areas.

Note: For training purposes, controlled substances may be stored at the Troop Headquarters K-9 Aid Storage Lockers with prior approval from the Troop Commander. These controlled substances shall be inspected and audited in accordance with the guidelines of this policy.

Guidance for Unusual Value or Size

The CEL of jurisdiction and/or the NIU Commander shall be called immediately for instructions and assistance when:

- Seized controlled substance evidence is too large to fit in the temporary Controlled Substance Evidence Locker; and
- When any marijuana plants are seized.

Controlled Substance Storage Area, continued

The ECP Officer shall:
Make arrangements with the NIU and/or the CEL of jurisdiction for the storage of items of significant value or unusual size that meet the following criteria:

Narcotics	Quantity
Marijuana	50 pounds or more
Cocaine	18 grams or more
Heroin	18 grams or more
Tablets/Pills	Approximately 1000 or more of Class A, B or C
Fentanyl	18 grams or more
Methamphetamine	18 grams or more

Controlled substances that appear to meet the above criteria shall:

- Not be held for more than seventy-two (72) hours at any Temporary Controlled Substance Evidence locker or CEL unless authorization is granted by the NIU Commander;
- Be documented on the appropriate forms/reports as "An Undetermined Amount of a Suspected Controlled Substance Pending Official Documentation from the Massachusetts State Police Crime Lab (M.S.P.C.L); and
- Be stored at the NIU Bunker at General Headquarters. If possible, the controlled substance should be submitted to the Crime Laboratory for analysis prior to being secured at the NIU Bunker.

The ECP Officer or Investigating Member shall:

- Notify the NIU or CEL forthwith to make arrangements for the transportation of the controlled substances according to NIU procedures.

Chain of Custody

Change In the Chain of Custody

The Investigating Member shall:

- Complete the SP 295; and
- Ensure the SP 295 is attached to controlled substances involved in a temporary change of possession outside the custody of the Station/Section/Unit ECP Officer.

Any change in the chain of custody of controlled substances shall:

- Be considered when controlled substances are required at judicial proceedings and are transferred to the Investigating Member from the Station/Section/Unit ECP Officer, CEL or NIU;
- Have entries made on the SP 295 and in the Temporary Controlled Substance Evidence Locker Journal (if applicable). In the event that additional space is required to accommodate entries on the SP 295 , additional SP 295's shall be used and recorded as "Page 1 of 2, Page 2 of 2 etc."; and
- Require copies of the SP 295 be retained and distributed as indicated on the form.

Chain of Custody, continued

Handling or Transporting Controlled Substances

Each time controlled substances are handled or transported, members shall:

- Ensure the presence and condition of the controlled substance by examining the material without opening closed containers or breaking any seals;
- Obtain the signature of the receiving party; and
- Document the date and location on the SP 295.

Inspection of Control Substance Packaging

All members involved in the movement of controlled substances at either the Station/Section/Unit, CEL or, NIU level shall:

- Inspect the packaging for signs of tampering; and
- Immediately notify the Station/Section/Unit Commander and the NIU Commander if the packaging appears to have been tampered with.

The Station/Section/Unit Commander shall:

- Notify through channels the Division of Standards and Training and request that an investigation be conducted.

Control Substance Packaging Opened

When any controlled substance evidence is opened during a court proceeding:

- A SP 655 Court Order to Open Secured and Closed Narcotic Evidence form shall be generated and kept with the opened evidence;
- The SP 655 shall include the name of the judge who requested it to be opened; and
- The SP 655 shall be signed by the Presiding Judge that ordered the evidence opened, or by either the Assistant District Attorney (ADA), or the Clerk Magistrate of the Court.

Note: The ECP Officer may complete the SP 655, however it shall only be signed by a judge, ADA, or clerk magistrate.

Inspections

Troop/Section/Unit Commanders shall:

- Conduct monthly line inspections of all Temporary Controlled Substance Storage areas under their control to ensure compliance with journal entries and access controls.

The NIU shall:

- Annually, or as directed by the Office of the Colonel/Superintendent, conduct official, unannounced, and random inspections of all Department Permanent Controlled Substance Storage Lockers to ensure compliance;
- Issue a written report with its findings and observations regarding the inspection conducted;
- Send a copy of this report to:
  - The Troop/Station/Section/Unit Commander (if applicable),
  - The supervisor of the CEL inspected; and
  - The NIU Commander

The Office of Professional Integrity and Accountability (OPIA) may:

- Conduct periodic checks of all Department Controlled Substance Lockers to ensure integrity of the system.

Subject: **Controlled Substance Intake-Storage**	Number: **INV-11**

Training

Station/Section/Unit ECP Officers, CEL and NIU personnel may:

- Be required to attend specified training conducted by the NIU Commander; and
- Include classroom and/or online academy training.

Audits

Whenever a new ECP Officer or Assistant ECP Officer is designated, an audit of controlled substances held in the temporary or permanent storage areas shall be conducted jointly with the outgoing and incoming ECP/Assistant ECP Officer. The results shall be documented in the Daily Administrative Journal. In the event no controlled substances are present due to a chain of custody transfer to the NIU, said audit shall document same.

References:

MGL c.94C, §47A;
MGL c.22C, §45, §46;
MPAC 84.1.1, 84.1.2, 84.1.4, 84.1.6;
SP 295 Drug Submission Form;
SP 655 Court Order to Open Secured and Closed Narcotic Evidence.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**INV-11A**

Subject:

Evidence/Contraband/Property Intake-Storage

Policy

The Department shall establish procedures for all evidentiary, found, seized, recovered, impounded, abandoned, or unclaimed property including contraband held within its custody to preserve the integrity of the Department and its personnel. A written incident report shall document the circumstances by which said evidence/contraband/property (ECP) came into the Department's possession and detail each item including the submission of affiliated evidence/property forms.

All ECP that comes into the possession of a member shall be entered into the ECP control function prior to the end of the member's shift, unless exigent-documented circumstances prevent the return, or entering, of said ECP. In the event of an exigent-documented circumstance, the ECP shall be entered in at the next most practicable time. Such delay and the steps taken to safeguard the ECP in the intervening time shall be documented in the incident/investigative report. A descriptive inventory of the ECP shall be made verbally to, and documented in the Daily Administrative Journal (DAJ)/ACISS log by the Troop Duty Officer, who shall be the approving authority for any documented delay.

All levels of supervision shall ensure compliance with established procedures within this policy regarding processing, storage requirements, and audits/inspections.

Controlled substance seizure procedures shall adhere to INV-11 Controlled Substance Intake-Storage.

Currency seizure procedures shall adhere to INV-14 Seized Currency.

Definitions

Chain of Custody: The record documenting the location and person in control of evidence/contraband/property from the time of its collection to final disposition.

Contraband (excluding controlled substances): May be property that is not in and of itself unlawful for a person to acquire or possess; however may have been acquired by the Department because of its use in an unlawful activity or manner, because of its nature, or due to circumstances surrounding the person who acquired or possessed it.

Note: Contraband in these instances shall be evidentiary and documented when applicable according to *INV-10 Evidence Collection and Preservation*.

Definitions, continued

Evidence/Contraband/ Property (ECP): Items in the possession of the Department to be held in a secure manner. Includes all evidence, contraband, found, unclaimed and abandoned property.

ECP Custodian: Station/Section/Unit Commander responsible for receiving, storing, maintaining, releasing, and accounting of all evidence, contraband, found, unclaimed and abandoned property within their facility.

ECP Temporary Storage: Temporary limited access storage area/locker within Department facilities for ECP that comes into the possession of the Department.

Evidence Room: Facilities used by the Department to store and preserve ECP in a secure manner with limited access.

Found Property: Non-evidentiary property in the custody of the Department which has been determined to be lost or abandoned and is not known or suspected to be connected with any criminal offense.

Unclaimed/Abandoned Property: Any property with no known owner in the custody of the Department.

Responsibilities

Position	Duties
Troop/Section Commanders	• Ensure the security and safeguarding of all ECP held in all Stations/Sections/Units under their command.
Station/Section/Unit Commander	• Shall be designated as the "ECP Custodian" of their Station/Section/Unit; • Shall be responsible for receiving, storing, maintaining, releasing, and accounting of all ECP in accordance with this policy; • May delegate the duties of the ECP Custodian to any member under their command and designate that member to serve as the "Assistant ECP Custodian" for that Station/Section/Unit; • When applicable, make arrangements with the appropriate facility for: o ECP testing or analysis; and o Firearms to be tested by the Department's Firearms Identification Section. • Shall transport, or designate the Assistant ECP Custodian to transport, any item requiring analysis or testing;

Responsibilities, continued

	• Ensure that members under their command are trained and familiar with the appropriate handling and storage of all ECP; and • Document in the DAJ/ACISS log all attempts to notify the owner or custodian of property in the custody of the Department if the property was not seized from the property owner or custodian.
Investigating Member	Upon arrival at the Station/Section/Unit the Investigating Member shall: • Provide the Desk Officer with a complete inventory of all ECP to be logged into the DAJ/ACISS log; • Log the ECP in the Temporary ECP Journal; • Firearms and other weapons shall be entered into the current evidence tracking system in use at time of seizure (BEAST, ACISS or other system), or if no electronic system is in use, entered into the Firearms journal. Prior to the end of their shift the Investigating Member shall: • Place each item into a Department Evidence bag and/or tag items individually that do not fit into Department Evidence bag(s); • Completely fill out all required information on Department Evidence bags or tags; • Secure ECP in the Temporary ECP Locker; • Attach a copy of the incident report to the ECP; • Property that comes into the possession of the Department that is of an exceptional, valuable and/or sensitive nature shall require additional security measures based upon the real and/or recognized value including alternative authorized temporary storage and/or Supervisory notification as necessary; • ECP Seized vehicles shall be documented utilizing the same reporting requirements as other evidence;

Responsibilities, continued

	• ECP that is too large to fit into the Temporary ECP storage locker may be given directly to the primary or assistant ECP Custodian with the transfer documented in the DAJ as a change in the chain of custody.

ECP Storage Area Provisions

Station/Section/Units ECP Permanent Storage

The ECP Storage Locker shall:

- Be locked and alarmed with limited access allowing for proper monitoring and security thus preventing unauthorized entry;
- Provide extra security measures for items of exceptional, valuable or sensitive items including, but not limited to firearms, evidentiary currency or jewelry; and
- Be maintained to prevent damage to ECPthat may occur due to moisture or extreme room temperature fluctuations.

Evidence/contraband shall:

- Be stored within a secure area inside the State Police facility of jurisdiction;
- Not be stored in vehicles or personal storage areas; and
- Perishable items requiring refrigeration, including blood and bodily fluids shall be secured within the facility's identified refrigerator. The refrigerator shall be in either the secured ECP Locker, or other area only accessible to authorized personnel.
- Vehicles seized as evidence or in conjunction with a civil forfeiture proceeding shall be stored in a secure manner to preserve evidence and prevent unauthorized access. Seized vehicles may be stored off-site from the seizing State Police facility, but shall be secured in an area with measures in place to maintain the evidentiary integrity, especially before/while being processed; including but not limited to: Secure locked fenced-in area, video monitoring, and/or on a limited access property such as another secure State Police facility. State Police Officers from the Station/Section/Unit seizing such vehicle(s) shall have full access to the vehicle(s) if held at a non-State Police facility; and
- Bicycles seized shall be stored either within the ECP Storage Locker or in a secure area or secured in a manner preventing unauthorized access.

Troop/Section Storage Area

Troop/Section Commanders shall:

- Maintain an ECP storage area within their Troop/Section Headquarters;
- The Troop/Section storage area shall be under the control of the Cases and Reports Supervisor; and
- The storage area shall be used to store ECP that has been forwarded and awaiting destruction or disposal.

Temporary Locker

Station/Section/Unit ECP Temporary Storage

Each Station/Section/Unit that stores ECP shall:

- Be provided with a Temporary ECP Locker with twenty-four (24) hour access to all authorized personnel providing limited access temporary storage of ECP including firearms;
- Any Station/Section/Unit without a Temporary ECP Locker shall secure evidence/contraband/property that comes into their custody at the barracks or Troop HQ of jurisdiction adhering to all MSP policy reporting requirements;
- Have a Temporary ECP Journal and Firearms Journal/tracking system to enter all pertinent information;
- Secure Firearms/weapons, ensuring that the firearm is safe and empty;
- Transfer evidence requiring refrigeration collected outside of the Massachusetts State Police Crime Laboratory (MSPCL) operating hours to the locked evidence refrigeration unit located in the Troop HQ of jurisdiction unless otherwise directed by a specialized unit Supervisor. This transfer shall be documented utilizing the appropriate chain of custody forms with notations in the DAJ of both the sending and receiving locations as well as notification to the evidence officer of the sending location;
- In the event that an item is too large to fit into the Temporary ECP Locker, the Investigating Member shall:
  - Consult with the primary or assistant ECP Custodian, their Supervisor or Troop Duty Officer to locate another secure location.
  - Notify the ECP of the alternative storage location if the ECP was not present to identify said alternative storage location.

Items secured in the Temporary ECP Locker shall have an entry made into the Temporary ECP Journal listing:

- Investigating Member's name;
- Investigating Member's ID number;
- Defendant's name(s);
- Defendant's date of birth;
- Case number;
- Date seized;
- Location where seized; and
- A description of the item(s) including the number of items.

Chain of Custody

Change In the Chain of Custody

When the ECP Custodian or Assistant ECP Custodian transfers evidence, contraband, property or firearms to an Investigating Member for judicial proceedings, or official Department proceeding, it shall be considered a change of possession within the chain of custody. Both the ECP Custodian/Assistant ECP Custodian and Investigating Member shall:

- Ensure appropriate entries are made within the ECP Ledger or Firearms Journal/tracking system and the DAJ/ACISS log; and
- Ensure all appropriate Department forms are completed indicating the change in possession.

Documentation of Chain of Custody

The Investigating Member shall:

- Ensure the appropriate chain of custody forms are completed for the examination of all physical evidence;
- Ensure the appropriate chain of custody form(s) accompanies evidence or contraband whenever it is involved in a temporary change of possession outside of the custody of either the ECP Custodian or Assistant ECP Custodian and/or the Investigating Member;
- Ensure that a record is made into the Station/Section/Unit's ECP Ledger or Firearms Journal/tracking system and DAJ identifying the new custodian; and
- Ensure the record identifies the ECP accordingly.

Inspection of Evidence or Contraband

All members involved in the movement of evidence or contraband at the Station/Section/Unit, shall:

- Inspect the packaging for signs of tampering; and
- Immediately notify the Station/Section/Unit Commander if the packaging appears to have been tampered with.

Chain of Custody Forms

- *SP 145 Chain of Custody: Evidence/Contraband /Property Form*: Used for all evidence (excluding controlled substances), contraband, found/unclaimed or recovered property to show the chain of custody of the item/property;
- MSPCL Forms;
- The following forms shall be used when necessary, retained and copies distributed as indicated:
  - *Evidence Submission Form:* Evidence or contraband requiring analysis; and
  - *SP 295 Drug Submission Form:* Controlled Substances requiring analysis.

Troop/Section Supervisor of Cases and Reports

The Troop/Section Cases and Reports Supervisor shall:

- Sign and date the Station/Section/Unit ECP Ledger as the final receiver of the property;
- Ensure a red line be drawn diagonally through the ledger entry to indicate final disposition and case closed;
- Destroy ECP in an appropriate and acceptable manner in the presence of another Commissioned Officer;
- Submit a written report, through channels, to the appropriate Troop/Section Commanding Officer or designee, listing the final disposition of all ECP; and
- Adhere to 19-SM-03 Procedures for Disposition of Evidence, Contraband, and/or Controlled Substances.

Property to be Auctioned

Pursuant to Massachusetts General Law c. 22C, § 45-46, the Department may:

- Sell held properties at a public auction; or
- Destroy held property; and
- Only sell or destroy held property after six (6) months when there is no proven ownership of the property.

The Department may select a vendor to hold the public auctions in accordance with established procedures. Information and instructions regarding the auction vendor and procedures shall be posted on PowerDMS under Bulletins-*Public Auction Vendor*.

Prior to the auction, Media Relations shall promulgate a notice per M.G.L. c. 22C, § 45, to the required media news outlets and newspapers that contain the following information:

- The time and place of the auction; and
- Description of the property to be auctioned.

Returning Property to Owner

When property is disposed or returned to an owner, specific information shall be recorded on the SP 145 and shall be:

- Attached (original) to the report and retained at the Station/Section/Unit;
- Forwarded (copy) to the EPC Custodian or Assistant EPC Custodian for filing; and
- Forwarded (copy) to the Troop/Section Supervisor of Cases and Reports and retained on file.

Office of Professional Integrity and Accountability Unit (OPIA)

The OPIA Unit shall conduct periodic audits of all Department ECP Storage Lockers to ensure the integrity of the system.

Audits & Inspections

ECP Custodian Change Audit

- When there is a change in the ECP custodian, an audit of the ECP under control of the Station/Section/Unit shall be conducted and documented. This audit is to be conducted jointly by the newly designated ECP custodian and a designee of the applicable Station/Section/Unit Commander to ensure records are current, properly annotated and include the random sampling of ECP for verification; and
    - During the joint audit associated with evidence custodian transfers, a sampling of the total amount of ECP requiring extra security measures (e.g., firearms, evidentiary currency, jewelry), and property and evidence items under the Station/Section/Units care must be reviewed concerning documentation and accountability.
    - The following table shall be utilized to ascertain the random sample size of ECP requiring extra security measures. Locate the total amount of high-risk ECP currently stored using the number under "Pieces of Extra Security Measures ECP." The corresponding "Required Sample Size" should be applied when conducting the respective audit. If the exact number for "Pieces of High-Risk ECP" is not listed, the following higher number should be used.

Pieces of Extra Security Measures ECP Held	Required Sample Size
100	92
250	203
500	341
1,000	516
1,500	624
2,000	696
> 2,500	30%

    - A random sampling of all other ECP items should be included in the audit. The number of selected items for the sampling of all items should be a number that should be sufficient to ensure the integrity of the system and accountability of property. The person assuming custody of the property and evidence should ensure that records are current and properly annotated. All discrepancies should be

Audits & Inspections, continued

documented and reported according to the reporting guidelines of this policy before the assumption of property and evidence accountability by the newly appointed custodian.

Note: If an error rate of more than 5 percent is discovered when conducting the extra security measure ECP audit, a complete inventory of the extra security ECP must be performed.

- The documented audit shall be maintained by the ECP custodian of the Station/Section/Unit and provided to the Station/Section/Unit Commander.

Annual Audit

Annually, the Troop/Section Commander shall assign a supervisor, not routinely or directly connected with the control of ECP, to conduct and document an audit of the ECP held by each Station/Section/Unit under their Command to ensure records are current, properly annotated and include the random sampling of ECP for verification. This audit shall follow the same guidelines audit guidelines listed above.

- The documented audit shall be provided to the Station/Unit ECP custodian and Station/Unit Commander.

Semi-Annual Inspections

- Every six (6) months Station/Section/Unit Commanders with secure storage area(s) for ECP shall assign the supervisor responsible for the ECP control function, or their designee, to conduct and document an inspection of the secure storage area(s). The inspection shall include an examination of the storage area(s) to assess if they are being maintained in a clean and orderly fashion; verify Department directives related to the property management system are being followed (proper handling, storage and record-keeping, etc.); verify the ECP is being protected from damage or deterioration; and that property having no further evidentiary value is being disposed of promptly.
  - The documented inspection shall be provided to the Station/Section/Unit ECP custodian and Station/Section/Unit Commander. Remediation of deficiencies, if warranted, shall be directed and documented by the Station/Section/Unit Commander.

Unannounced Inspections

- At least annually, every Station/Section/Unit with an ECP storage room shall direct an unannounced inspection of the room be conducted and documented by a designee not routinely or directly connected with control of the ECP. This inspection is not intended to be a full inspection; but should inspect for cleanliness, orderliness and trace a few pieces of ECP to verify they are in the proper location as stated in the ECP logs; and

    - The documented inspection shall be provided to the Station/Section/Unit ECP custodian and Station/Section/Unit Commander.
- The Office of the Colonel/Superintendent may direct unannounced, random inspections of ECP storage areas to ensure compliance with Department policies.
    - These inspections shall be documented and maintained by the Office of the Superintendent and the Division Commander of DST.

Record Maintenance

- With the exception of unannounced inspections directed by the Office of the Colonel/Superintendent, the Station/Section/Unit Commander shall maintain a record of all audits, semi-annual inspections and unannounced inspections in a centralized location.

Reporting

- Audits or inspections that reveal missing ECP shall be reported through channels to the Division Commander of DST immediately upon receipt of the information.

References: M.G.L. c. 22C, § 45 and § 46;
M.G.L. c. 94C, §. 47A;
Evidence Submission Form;
SP 295 Drug Submission Form;
SP 145 Chain of Custody: Contraband/Evidence/Property Form;
19-SM-03 Procedures for Disposition of Evidence, Contraband, and/or Controlled Substances;
MPAC: 84.1.1, 84.1.6, 84.1.7.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**INV-13**
Subject:	
Asset Forfeiture	

Policy

The Department shall adhere to state and federal forfeiture laws involving illegal activities.

Troop/Section Asset Forfeiture Officer

The Asset Forfeiture Officer (AFO) shall:

- Provide assistance to members regarding investigations when authorized by the Troop Duty Officer;
- Oversee forfeiture proceedings and manage seized assets until forfeited;
- Maintain a database and files of all seizures and forfeitures; and
- Act as a liaison with the Financial Evidence Officer (per INV-14 Seized Currency), and the Offices of the District Attorney, Attorney General, or U.S. Attorney.

Non-Field Services Sections/Units

This policy is applicable to all Department entities, except those assigned to the Offices of the District Attorney, Attorney General, U.S. Attorney, or a federal task force, and there is an internal mechanism for tracking such seized currency. Members shall follow the policy as set forth by that office or task force.

Troop/Section/Unit Commanders requesting to deviate from this policy shall forward written requests through channels to the Deputy Superintendent for approval.

Factors of Consideration

In some situations, one factor alone may be insufficient to justify a seizure and may require a combination of additional factors. Some factors are:

- Suspect is evasive, or gives implausible or false answers;
- Suspect has record of controlled substance charges;
- Suspect is carrying a large or unusual amount of currency;
- Suspect cannot explain where the currency came from, or what it is for;
- Suspect has a large sum of currency or an expensive vehicle and no means of income;
- Suspect denies ownership of currency;
- Currency is concealed in an unusual location; or
- A narcotics canine alerts on the currency, vehicle, or property.
  Note: A canine alert alone is not enough to establish probable cause for the seizure of currency.

Making a Seizure

Seizures may be made when there is probable cause to believe that the vehicle, currency, or other property is connected to the sale or distribution of controlled substances. This authority is allowed by Massachusetts General Laws (MGL) c.94C §47.

Members may seize currency when there is probable cause to believe that the currency is:

- Being used or was intended for use in the procurement, processing, delivery, or distribution of controlled substances;
- The proceeds of sales of controlled substances; or
- Involved in the furtherance of criminal enterprise.

Note: Currency seized shall be processed in accordance with INV-14.

Seizing a Vehicle

The Fleet Administrator has the authority to accept or reject vehicles on behalf of the Department. Any vehicle accepted by the Department, shall be delivered to the Fleet Section for inspection according to ADM-19.

A vehicle may be seized when…	A vehicle should not be seized if…
1. An operator, owner, or occupant of the vehicle is arrested for possession with intent to distribute or trafficking: • Ten (10) pounds or more of marijuana; • Any amount of heroin; • Any amount of cocaine; or • Other controlled substances, as outlined in M.G.L. c.94C, § 32A-G or 32I. 2. The owner knew or should have known that it was being used for such purposes.	• It is rented or leased (unless seized for evidentiary purposes); or • The owner had no knowledge that it was being used for illegal purposes. Note: The Troop AFO shall consult with the District Attorney's Office of jurisdiction and determine if there is a lien on the vehicle that an entity is willing to assume.

Use of Seized Assets

The Colonel/Superintendent may expend funds and proceeds from the Special Law Enforcement Trust Fund to:

- Defray the costs of extended investigations;
- Provide matching funds for grants; and
- Accomplish other law enforcement purpose(s).

Funds shall not be considered a source of revenue to meet operational expenses.

Troop Asset Forfeiture Process

Step	Action
1	The determination is made to seize the assets e.g., vehicle, currency, or other property.
2	All seized assets are to be secured according to Department policy.
3	The seizing member shall notify the Troop Duty Officer of the seizure.
4	The Troop Duty Officer shall notify: • The Troop AFO and may authorize call outs of the AFO after business hours; and • The Financial Evidence Officer of all currency seizures in accordance with INV-14.
5	The seizing member shall be assigned an incident/case number, complete a written report detailing the circumstances of the asset seizure, and prepare the necessary reports and forms.
6	The Troop AFO shall: • Confirm assets are secured with the investigating member; • Conduct an investigation to determine ownership and liens of the assets; and • Assist the Financial Evidence Officer.
7	If it is determined that the asset forfeiture proceedings shall not continue, the assets shall be returned, as soon as possible, to the lawful owner.
8	Motor vehicles seized shall be secured as directed by the Troop/Section Commander.

Subject:	Number:
Asset Forfeiture	**INV-13**

References: MGL c.94C;
MGL c.135, § 7, 8, 10, 11;
ADM-19 Vehicle Management;
INV-10 Evidence Collection/Preservation;
INV-11 Controlled Substance-Intake/Storage;
INV-14 Seized Currency;
TRF-09 Towing;
TRF-10 Vehicle Inventory;
A Guide to Equitable Sharing of Federally Forfeited Property for State and Local Law Enforcement, March 1994, US DOJ.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**INV-14**
Subject:	
Seized Currency	

Policy

The Department shall establish rigid controls and strict accountability for all seized currency coming into its custody. A non-interest bearing cashless system shall be utilized to ensure that all seized currency is properly accounted for, secured, stored, and readily retrievable. Any changes in the custody of any seized currency shall be appropriately documented.

Applicability

This policy is applicable to all Department entities, except under the following conditions:

- Members assigned to Offices of the District Attorney, Attorney General, U.S. Attorney, or federal task force are exempt from this policy; and
- If a documented internal mechanism exists for tracking seized currency, this policy does not apply.

Troop/Section/Unit Commanders requesting to deviate from this policy shall forward written requests through channels to the Deputy Superintendent for approval.

Seized Currency

Members shall not seize less than three-hundred ($300.00) dollars from a defendant unless the currency is seized as evidence.

Seized currency shall not include:

- Non-evidentiary currency received during custodial processing;
- Currency used for controlled purchases of contraband; or
- Currency that has independent forensic value. (i.e., currency stained with blood, bodily fluids, or other evidentiary material)

Seized currency shall be processed at the appropriate sub-station in the Troop of jurisdiction.

Any seized currency that may be contaminated with any biological hazard, dangerous drugs, or chemicals shall be clearly labeled to warn of the threat. Any members handling potentially tainted currency shall utilize proper protective equipment to minimize the risk of exposure. Any other agency or entity who will handle the seized currency shall also be warned of the threat in writing by the member transferring the currency.

Responsibilities

Position	Duties
Desk Officer	• Visually observe currency drop safe at the start of shift for general condition and make entry into Daily Administrative Journal (DAJ)/ACISS system; • Make appropriate entries into DAJ system upon seizure and retrieval; • Assign a case/incident number to the Investigating Member; and • Notify Troop Duty Officer of the seizure and provide the RAMS or ACISS case number and the Investigating Member's name, ID number, and current duty assignment.
Investigating Member	• If practicable, when a member locates currency to be seized, they will immediately request another member or Law Enforcement Officer to act as a witness; o When no such witness is available, the member shall contact the appropriate Troop Duty Officer of jurisdiction requesting a DAJ entry be made; • If practicable, the packaged and labeled currency should be photographed on scene; • Return directly to the barracks of jurisdiction to process the seized currency in accordance with this policy; • Photograph or photocopy currency for evidentiary purposes, if feasible; • Currency will not be counted at the time of the seizure; • Package and seal currency in a Department evidence bag (evidence bags shall be labeled 1 of 1, 1 of 2, 2 of 2, accordingly), ensure both members initial the seal, ensure both members sign bag with ID numbers, include the corresponding RAMS or ACISS case number, and the notation, "An Undetermined Amount of U.S. Currency Pending an Official Count"; • When the currency is seized from a particular individual, the member will issue the individual an SP 418 Seized Custody Receipt with the notation, "An Undetermined Amount of U.S. Currency Pending an Official Count." If the individual refuses to sign the receipt or if the member determines that it is tactically unsound to allow the individual to sign, this fact will be noted on the receipt and in the member's corresponding report of the seizure;

Responsibilities, continued	Investigating Member, continued	• Prepare an SP 417 Currency Custody Form with the notation, "An Undetermined Amount of U.S. Currency Pending an Official Count"; • Deposit Department evidence bag with attached SP 417 Currency Custody Form and SP 418 Seized Currency Receipt into currency drop safe with witnessing member present; • File copies of SP 417 and SP 418 with the Station Commander and ensure copies are attached in the appropriate case file; and • Complete an incident report detailing the circumstances of the seizure.
	Troop Duty Officer	• Notify the Financial Evidence Officer by email of the seizure; • Make appropriate DAJ entries; and • Ensure an electronic copy of the GHQ Finance Section Bank Sweep Account deposit slip (as provided by the Financial Evidence Officer) is included in the appropriate case file.
	Financial Evidence Officer	• In the presence of another Commissioned Officer, retrieve seized currency from the currency drop safe, no later than next banking business day or as otherwise authorized by the Troop Commander; • Document any change in Custody on SP 417; • The seized currency should be photographed at this time using the Department issued camera in each barracks; • Ensure appropriate DAJ/ACISS entries are made; • In the presence of another Commissioned Officer, transport the seized currency to a local banking institution designated by the GHQ Finance Section; • Both Commissioned Officers will be present when the Department evidence bag(s) is/are unsealed and will witness the official count at the financial institution. The evidence bag(s) should be cut open at the bottom to remove the currency while preserving the bag(s) with the seals, initials, and signatures intact. The Financial Evidence Officer will maintain the original evidence bag(s) in his/her files; • Deposit currency into a cashless system (GHQ Finance Section Bank Sweep Account) on the same banking business day as retrieved; • Enter the amount of the seizure into the approved accounting program;

Responsibilities, continued

Financial Evidence Officer, continued	• Notify the Troop Commander, Troop Duty Officer, and the Investigating Member of the official count and ensure appropriate DAJ/ACISS entries are made; • Provide a copy of the deposit slip and any other related relevant documents that may exist (i.e., denomination breakdown) to the Investigating Member for electronic inclusion in the appropriate investigative case file; • Send copies of the SP 12 Incident Report to the Chief Financial Officer (CFO) of the District Attorney's Office of jurisdiction; • Maintain copies of SP 12s, SP 417s and SP 418s in a dedicated folder filed alphabetically and by year; • Copies of SP 417, SP 418, deposit slip/receipt should be provided electronically to Finance Section via MSPForfeiture@pol.state.ma.us; and • File open and closed cases separately.
Station Commander	• Maintain copies of SP 417 and SP 418 for inspections.
Troop Commander	• Maintain a book of deposit slips (in duplicate) for the GHQ Finance Section Bank Sweep Account. Deposit slips may be obtained from the Finance Section, Director of Finance. A two to three week advance order time is needed. • Assign a Commissioned Officer as the Financial Evidence Officer; • Maintain historical records of members provided with combination access; • Change access combinations as required; • Conduct and document quarterly audits; • Conduct investigations as appropriate; • Notify the Division Commander of any discrepancies; and • Upon appropriate request, forward a To/From to the Finance Section requesting return of seized funds.

Official Count

The final official amount shall be determined by the GHQ Finance Section Bank Sweep Account financial institution of deposit.

Troop/Section Commanders shall document and investigate any currency discrepancies that cannot be reconciled and report findings to the Division Commander.

Return of Seized Funds

Any person requesting the return of seized currency shall:

- Request the return in writing to the Troop Financial Evidence Officer; and
- Provide a copy of the court order, if applicable.

The respective Troop Commander or designee shall forward a To/From to the Finance Section requesting a refund.

Disposition of Currency

If no person makes a valid claim to found, unclaimed, or abandoned currency within six (6) months from the date the currency was turned into the Department, the funds shall be forwarded to the State Treasurer via the Department's Finance Section.

Prior to forwarding the funds to the State Treasurer, the Department may deduct all reasonable charges and expenses incurred in connection with the deposit and accounting of the currency. Such deductions shall be made by the Department's Finance Director and documented accordingly. Any claim for return of found, unclaimed, or abandoned currency after the funds have been forwarded to the State Treasurer, shall be made to the State Treasurer's Office.

All original documents relative to seized currency ordered forfeited through legal proceedings shall be forwarded to the Finance Section for the Special Law Enforcement Trust fund within sixty (60) days of adjudication.

Accounting and Audits

The Financial Evidence Officer shall maintain:

- Copies of documents relative to seized currency ordered forfeited through legal proceedings;
- A Department approved software accounting system;
- SP 12s, SP 417s, and SP 418s for currency received and records, documentation, or invoices of currency disbursements, including the financial institution where seized funds were deposited;
- Prior to any change of command of the Troop/Section/Unit Commander, Executive Officer, or Financial Evidence Officer, there shall be a documented reconciliation of the accounting records and current balances with the incoming member(s);
- A documented internal audit of all seized currency accounting records and practices shall be conducted annually by the appropriate Division Commander; and
- An audit of seized currency may be conducted as directed by the appropriate Division Commander or the Colonel/Superintendent.

Reports

Troop/Section/Unit Commanders shall:

- Submit a quarterly report from the approved accounting program to their Division Commander (due January 10, April 10, July 10, and October 10); and

Reports, continued

Submit a copy of the quarterly summary/statement for funds processed to the Chief Financial Officer (CFO) of the District Attorney's Office of jurisdiction and to the Finance section via MSPForfeiture@pol.state.ma.us.

Large/Bulk Seizures

For large/bulk seizures of currency that cannot fit into the the Currency Drop Safe, the Investigating Member shall immediately:

- During normal business hours notify the Troop Duty Officer to arrange for the Troop Financial Evidence Officer take possession of the currency for bank deposit in accordance with this policy; or
- Outside of normal business hours business hours, notify the Troop Duty Officer who shall notify the NIU Commander or designee to make arrangements for the transportation of the seized currency to the NIU bunker at General Headquarters in Framingham.

Currency Drop Safe

Currency drop safes shall be located and maintained at each sub-station as determined by the Division Commander. Only the Troop Commander, Executive Officer, and Financial Evidence Officer shall have authorized access to the currency drop safe and combinations. Whenever the currency drop safe is opened:

- Two (2) members shall be present at all times; and
- Access and retrieval information shall be entered into the station DAJ.

Drop Safe Combinations

Troop Commanders shall be responsible for the change of safe combinations under their command.

Whenever there is a change of command, transfer, or departure of a Troop Commander, Executive Officer, or Financial Evidence Officer, the access combination shall be changed.

References

INV-13 Asset Forfeiture;
SP 12 Incident Report;
SP 417 Currency Custody Form;
SP 418 Seized Currency Receipt;
MPAC: 84.1.1.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**INV-15**
Subject:	
Field Interview and Observation Reports	

Policy

Members shall follow the established guidelines for the collection, security, and dissemination of information gathered through field interviews and observations.

Definitions

SP 73 Field Interview and Observation Report (FIO): An internal, Department report that documents information about a person, place, vehicle, event, occurrence, or any other known activity, observed by a Department member, that may be linked to suspicious or criminal activity or may be of interest to the law enforcement community.

Collection of Information

Information may be recorded on a SP 73 or any other format that is approved by the Criminal Information Section (CIS).

FIO reports are an important crime prevention and information gathering resource. Analysis of these reports is a valuable aid to investigators in uncovering leads that may result in the solving of crimes and the apprehension of criminal suspects.

The collection of information for FIO reports shall not be based solely on an individual's or group's:

- Support of a particular cause;
- Race;
- Color;
- Religion;
- Gender;
- National origin or ancestry; or
- Political affiliation.

Members collecting information for FIO reports shall not:

- Conduct random stops of persons or vehicles to gather information; or
- Employ or direct an individual to engage in any illegal activities.

Subject:	Number:
Field Interview and Observation Reports	**INV-15**

Public Contact

Members are encouraged to:

- Collect as much information based upon their own observations; and
- Gather as much information provided to them on a voluntary basis.

Members may:

- Detain a person or vehicle briefly when there is reasonable suspicion of criminal activity; or
- Stop and frisk a subject's outer garments for weapons when articulable facts or circumstances warrant such action, for the safety of the public and the member.

A person stopped by a member, who refuses to cooperate or answer questions, shall not be further detained without reasonable suspicion or probable cause.

SP 73 Field Interview and Observation Reports

FIO Reports should be accessible by every member while on duty. Additionally:

- Members should complete a report whenever a known criminal is observed or a person, place, vehicle, event, occurrence, or any other activity is observed that would indicate criminal activity or potential criminal activity;
- A separate FIO Report shall be completed for each member of a group and for each observation made; and
- Information shall be typed or printed in black ink and its content should be as complete as possible.

Procedures for completed FIO Reports:

- Provide a copy of the FIO to the Troop/Section/Unit of jurisdiction;
- Forward the original hard copy of the FIO Report to CIS; and
- If the information within the FIO Report is related to terrorism or homeland security contact:
  - CIS during normal business hours; or
  - The Communications Section OIC other than normal business hours.

Security and Retention

FIO Reports shall be secured at all times by CIS. A dissemination log shall be maintained for all requests for review and dissemination of information.

Subject:	Number:
Field Interview and Observation Reports	**INV-15**

Dissemination

Requests for information from the FIO database shall be made to the Commanding Officer of the CIS.

CIS shall only disseminate FIO information:

- In the furtherance of an authorized law enforcement activity;
- To authorized law enforcement or criminal justice personnel; and
- On a "need-to-know" and "right-to-know" basis per INV-08 Criminal Intelligence.

After review by either CIS, or the Communications Section OIC, information contained within an FIO Report determined to be critical, time-sensitive, or pertaining to public or officer safety shall be disseminated to law enforcement agencies, as appropriate.

Responsibilities

Requests for dissemination shall include the:

- Date and time of the request;
- Requesting Officer's name, rank, identification (ID) number and agency;
- Case number or reason for the request; and
- Name of the person(s) or incident(s) and information sought.

The CIS shall:

- Respond to requests for information from FIO Reports; and
- Document requests and dissemination of information.

References: INV-08 Criminal Intelligence;
MPAC: 1.2.3.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**INV-16**
Subject:	
Electronic Recording of Interrogations	

Policy

Members shall, whenever it is practical, electronically record all custodial interrogations of suspects or interrogations of suspects conducted in places of detention.

Case Law

In *Commonwealth v. DiGiambattista*, 442 Mass. 423 (2004), the Supreme Judicial Court held that if the prosecution introduces a confession or statement that the police obtained during an interrogation of a defendant, who was either in custody or at a place of detention, and the police did not electronically record the statement, the defendant is entitled to a cautionary jury instruction.

Upon the defendant's request, the judge must instruct the jury that the State's highest court has expressed "*a preference that such interrogations be recorded whenever practicable and . . . that, in light of the absence of any recording of the interrogation in the case before them, they should weigh evidence of the defendant's alleged statement with great caution and care*." This jury instruction is required regardless of the reason that the police did not record the interrogation.

Definitions

Custody: Circumstances in which a reasonable person would believe that their freedom of action has been curtailed such that they are not free to leave.

Electronic Recording: Preservation of an interview/interrogation through the use of audio or audio/video recording equipment.

Interrogation: Occurs when an officer's questions, actions or words (other than those normally attendant to arrest and custody), are designed to elicit an incriminating response from a suspect.

Place of Detention: A secure facility where persons may be held in detention in relation to a criminal charge(s) (e.g., a state police barracks, prison, jail, a department of youth services secure facility).

Definitions, continued

Suspect: A person who has either been charged with a crime or a person for whom there is a reasonable basis to believe that they may in the future be charged with a crime. Witnesses, victims, and other persons who provide information to a member are not considered suspects, unless and until, there is reasonable basis to change their status.

Applicability

These guidelines require members to record, whenever it is practical, two (2) types of interrogations:

1. Custodial interrogations of suspects; and
2. Interrogations of suspects occurring at places of detention.

Wiretap Violations

The Massachusetts wiretap statute, Massachusetts General Laws (MGL) c. 272, § 99, generally prohibits anyone from secretly recording another person's oral statements. Accordingly, unless one of the narrow exceptions in the wiretap statute applies, a member who electronically records a suspect's interrogation shall do either of the following:

- Notify a suspect that their statements are being recorded; or
- Conduct the interrogation in such a way that it is obvious to the suspect that their statements are being recorded.

When the suspect knows, or reasonably should know, that they are being recorded, the member may record the interrogation without explicit consent to do so.

Creating a Clear and Complete Record

To the extent it is practical members should electronically record the entire interrogation of a suspect. To assist in the creation of the record, members shall do the following:

- Ensure that the recording device is functioning properly;
- Start the recording device;
- Inform the suspect that they are being recorded unless it is otherwise obvious;
- State the date, time, location, and names of persons present. If a video recording device is used which imprints the time on the tape or disk, verify that the correct time is displayed;
- State the full name of the suspect;
- Execute appropriate Department forms including Miranda warning and waiver, and waiver of prompt arraignment (if applicable);

Creating a Clear and Complete Record, continued

- If the member must suspend the recording for any reason, they shall make a record of:
  - The reasons for stopping (i.e., taking a break or a malfunction);
  - The time the recording device is turned off;
  - The time it is turned back on; and
  - What transpired while the recording device was turned off.
- If the member uses or refers to documents or other items during the interrogation, the member shall describe those documents or items on the record and mark them with a unique number (similar to an exhibit number at trial) and the member's initials. If the member is unable to write on the actual document or item, the member may write on a bag, envelope, or case in which the document or item is placed, or on a piece of tape which can be attached to the document or item; and
- Conclude the recording by stating the date and the time the interrogation is completed.

Suspect Refuses to be Recorded

Refusal Given Before the Recording Device is Activated:

- If it is practical, turn on the recording device to record the refusal;
- Identify the lead member and the suspect then state the date, time, and location, inform the suspect of any applicable rights and inform the suspect of the benefit to recording, including the fact that a recording will create a clear and complete record of what was said to the suspect, and what the suspect said during the interrogation;
- Ask the suspect on the record if they are willing to make an electronically recorded statement;
- Advise the suspect if, at any time, they change their mind and decide that they do want the interview to be recorded, they should let the member know and the member shall turn on the recording device; and
- If the suspect still refuses, turn off the device, execute a signed refusal form SP 609 Refusal Form, and proceed with the interview.

Suspect Refuses to Have Their Refusal Recorded

- Advise the suspect of the benefits of electronically recording any communications;
- If the suspect objects to having their refusal electronically recorded the member shall execute a SP 609; and
- The member may proceed without recording the refusal or the interrogation.

Suspect Refuses to be Recorded, continued

Suspect Refuses After the Recording Device is Activated

- If, during the course of a recorded interrogation, a suspect decides that they no longer want to answer questions unless the recording device is turned off, the member shall again advise the suspect of the benefits of recording the interrogation; and
- If the suspect still refuses, the member shall turn off the recording device execute a SP 609 and proceed with the interview.

Discretionary Decision Not to Record

A member may decide not to record an interrogation, even where it is practical to do so, if that member believes that:

- Recording the interrogation will jeopardize the safety of a member, the suspect, or any other person; or
- It is ill-advised under the circumstances to record the interrogation.

If a member decides not to record an interrogation, even where it is practical to do so, based upon the above factors, the member shall document in the case report, the reason(s) why the interrogation was not recorded.

Recording Devices

The member should choose a recording device that has removable media (e.g., tape, disk, memory card, etc.) which can be easily duplicated.

Recording Device Malfunctions

If the recording device malfunctions, the member conducting the interrogation shall make a decision whether and how to continue the interrogation and shall document what occurred.

If the recording device can be restarted or replaced immediately:

- State on the record that the device malfunctioned;
- State how long the device was not working, and
- Whether or not the suspect made any statements that were not recorded.

If the recording device cannot be restarted or replaced immediately:

- Include in the interview or case report the fact that the device malfunctioned;
- Ask the suspect whether they wish to continue the interrogation without a recording device, or whether they wish to suspend the interrogation until an operable recording device is available;

Recording Device Malfunctions, continued

- If the suspect consents to continuing the interrogation without a recording device, document the consent and the interrogation in some manner, such as in a signed written statement by the suspect or in the member's interview or case report; and
- Note whether or not the suspect made any statements that were not recorded.

Inoperable or Unavailable Recording Device

If there is no recording device available or the recording device is inoperable, the member should:

- Ask the suspect whether they wish to continue the interrogation without a recording device or suspend the interrogation until an operable recording device is available.

If it is impractical to defer the interrogation, and the suspect consents to continuing the interrogation without a recording device then:

- Include in the interview or case report the fact that no recording device was available; and
- Document the consent and the interrogation in some manner, such as in a signed written statement by the suspect, or in the member's interview, or case report.

If, under the circumstances, it is impractical to seek or obtain the suspect's consent to continuing the interrogation without a recording device, the ultimate decision to continue shall be made by the member on a case-by-case basis.

Preservation and Copying of Original Recordings

The member who conducted the interrogation shall preserve the original recording. Preservation steps include:

- Remove the storage medium from the recording device;
- Clearly label and appropriately store recordings and copies;
- If the interrogation is recorded digitally, the member shall preserve at least one (1) whole copy of the original recording file;
- As soon as it is practical, create at least one (1) exact copy of the original recording;
- Clearly label copies as such;
- Use copies, not original recordings, to make additional copies; and
- Copies, not the original, shall be used to prepare a written transcript, to comply with discovery obligations, and for all other purposes.

To the extent it is practical, statements from multiple suspects should not be recorded on the same tape or disk.

Storage

The member shall preserve all written forms, notes, or records of all statements by a suspect that were not electronically recorded in the original case file.

All electronically recorded interrogations shall:

- Be preserved according to the state records retention law and Department policy as criminal evidence; and
- Be stored in such a manner so as to easily differentiate between original recordings and copies.

Each original and copy shall be authenticated by the interrogator with the following information:

- Date and time of recording;
- Location of the interrogation;
- Name of person interrogated;
- Name of person(s) conducting the interrogation; and
- Departmental assigned case number or incident report number.

References: SP 609 Refusal Form;
MGL c. 272, s.§ 99;
Commonwealth v. DiGiambattista, 442 Mass. 423 (2004).

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**INV-16A**
Subject:	
Eyewitness Identification	

Policy

The Department recognizes the importance of conducting and documenting eyewitness identification information in accordance with established guidelines, while recognizing that members are free to exercise discretion in adapting these guidelines to fit the unique circumstances of each case.

Eyewitness identification frequently plays an important role in Department investigations, and it is critical that eyewitness evidence be accurate and reliable in order to ensure that the highest possible quality of evidence is obtained.

Members conducting eyewitness identifications shall take steps to ensure that witnesses/victims are separated during the identification processes in the event multiple witnesses/victims are present simultaneously.

Members conducting eyewitness identifications shall follow reporting requirements including, but not limited to, documenting the process in an incident/investigative report.

Definitions

Blind Administration Procedure: A procedure during which the officer/investigator who conducts the lineup has no knowledge of who the suspect is, which reduces unintentional influences. **Whenever practical, this method should be used**.

Field Identification (Show-Up): An eyewitness identification procedure in which a single suspect is viewed by an eyewitness shortly after the commission of a crime for the purpose of identifying or eliminating a suspect in a criminal offense.

Filler: A person or photograph used in an eyewitness identification procedure not suspected of the offense but generally meets the description of the suspect.

Live Lineup: An eyewitness identification procedure in which the witness to a criminal offense is asked to identify one suspect from a group of persons.

Photo Lineup/Photo Array: An eyewitness identification procedure in which the witness to a criminal offense is asked to identify one suspect from a group of photographs.

Definitions, continued

Relative Judgments: Relative judgments occur when witnesses encounter a lineup in which the actual perpetrator is not in the lineup (i.e., the suspect is not the actual perpetrator). Research has shown that eyewitnesses tend to select the person who looks most like the perpetrator relative to other lineup members because they presume that the actual perpetrator will be in the lineup.

Sequential Identification Procedures: Sequential identification is a procedure where an eyewitness views only one member of a lineup or one photograph at a time. The witness must make a determination as to whether they can make an identification on each lineup member or photo before viewing the next lineup member or photo.

Simultaneous Identification Procedure: Simultaneous identification is a procedure that displays a group of individuals or group of photographs to a witness at the same time. This allows the witness to compare all individuals or photographs before determining if they can make an identification.

Guidelines and Eyewitness Advisory

Before any eyewitness identification procedure is conducted, members shall administer an eyewitness advisory, utilizing the SP 645 Eyewitness Advisement. The advisory provides clear, consistent, and forceful instructions to avoid relative judgment or any prejudicial action that may influence the witness.

The Massachusetts Supreme Court held in Commonwealth v. Silva-Santiago, 453 Mass. 782 (2009), that a photo array procedure was not per se suggestive where the police failed to use the standard advisements, sequential presentation, or a blind presenter. However, the court stated that it expects such procedures, especially the standard advisements, to be used in all future identification procedures.

Department members shall adhere to these guidelines and utilize the appropriate Department forms (see References) when conducting any eyewitness identification procedure, except for the following conditions:

- If the members are assigned to Offices of the District Attorney, Attorney General, U.S. Attorney or federal task force; and
- An internal mechanism exists for conducting eyewitness identification procedure.

Field Identification (Show-Up)

Members should document the circumstances warranting field identification according to SP 646 Show-Up Identification Procedure, which may include:

- The time and place of the crime;
- Factors matching witness description;
- Factors attracting police attention; or
- Exigent need including public safety and quick and/or efficient police investigation.

If multiple witnesses are involved, separate the witnesses and instruct them to avoid discussing details of the incident prior to the field identification.'

Whenever possible, the victim/witness should be transported to the location where the subject is located.

Members may assist in transporting witness(es) to the show up.

The subject may be transported to the victim/witness location under extenuating circumstances. In such instances, the subject should be transported in an unmarked vehicle, if available, to the victim/witness location. If possible, the subject should be transported in the front seat of the vehicle. If the subject is handcuffed, an effort should made to conceal the handcuffs.

Photo Lineup/Array

Whenever practical, members shall use a blind administration to present the photo lineup to the witness. Members shall:

- Utilize form SP 645 to administer the Eyewitness Advisory;
- Avoid saying anything that may influence the witness's selection;
- Use either the sequential or simultaneous presentation procedure;
- Show all the photographs to the witness even if identification is made when using the sequential procedure;
- Have the witness initial and date the photograph chosen if identification is made; and
- Record or document the victim/witness statement of certainty.

Members may use audio and/or video recording as necessary to memorialize the administration of the lineup/array. When utilized, the record(s) shall be maintained as part of the case file.

Advise victim/witness of the recording before proceeding and document in writing utilizing SP645 or on the recording their acknowledgement of the recording device(s).

Photo Lineup/Array, continued

To compose a photo lineup, consider the following:

- Select eight photographs;
- Include only one suspect in each array. The photo of the suspect may not unduly stand out;
- Select seven fillers who generally fit the given description of the suspect;
- Identify each photograph with a letter or number;
- Document the assigned letter/number and the name and date of birth of the subject of each photograph in a location not in view of the witness;
- Avoid using fillers that so closely resemble the suspect that a person familiar with the suspect might find it difficult to distinguish the suspect from the fillers;
- Create a consistent appearance between the suspect and fillers with respect to any unique or unusual feature (scars, tattoos, etc) used to describe the suspect by artificially adding or concealing the feature;
- Ensure that no identification or criminal information pertaining to the suspect or filler photographs is visible to the witness; and
- Document the name, police department and identification number of the officer who prepares the photo lineup.

Live Lineup Procedure

Whenever practical, members shall use the blind administration process to present a live lineup to the witness.

Members shall:

- Utilize form SP645 to administer the Eyewitness Advisory;
- Avoid saying anything that may influence the witness's selection;
- Use either the sequential or simultaneous presentation procedure;
- Show all the individuals to the witness even if identification is made when using the sequential procedure;
- If identification is made, have the witness initial and date the appropriate paperwork; and
- Record or document the victim/witness statement of certainty.

To compose a live lineup consider the following;

- Select six individuals;
- Use only one suspect in each live lineup;
- Select five fillers who generally fit the description of the suspect;
- The suspect must not unduly stand out;
- Identify each individual with a letter or number;
- Document the assigned letter/number and the name and date of birth of each individual in a location not in view of the witness;
- Ensure that no identification or criminal information pertaining to the suspect or filler is visible to the witness; and
- Document the name, police department and identification number of the officer who prepares the live lineup.

Live Lineup Procedure, continued

Members may use audio and/or video recording as necessary to memorialize the administration of the lineup/array. When utilized, the record(s) shall be maintained as part of the case file.
Advise victim/witness of the recording before proceeding and document in writing utilizing the SP 645 or on the recording their acknowledgement of the recording device(s).

References

U.S. Department of Justice, (1999) Eyewitness Evidence, A Guide for Law Enforcement; Improve the Investigation and Prosecution of Cases in the Criminal Justice System;
Commonwealth v. Silva-Santiago, 453 Mass. 782 (2009);
SP 644 Eyewitness Identification Form;
SP 645 Eyewitness Advisement;
SP 646 Show-Up Identification Procedure;
MPAC: 42.2.11, 42.2.12.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**INV-17**

Subject:

Travel/Immigration Status Inquiries and Investigations

Policy

Investigating and enforcing violations of federal immigration law is not a mission of the Massachusetts State Police. Accordingly, it is not appropriate for a member of the State Police to inquire about a non-citizen's immigration or travel status for the sole purpose of facilitating that person's detention or deportation by U.S. Immigration & Customs Enforcement (ICE).

However, a member of the State Police may inquire into a person's immigration or travel status if the inquiry is part of, and reasonably likely to facilitate, the investigation of a violation of state law, federal criminal law (excluding federal immigration law), or conduct independent of immigration status that poses a threat to public safety or order. A member of the State Police may also notify federal authorities of the imminent release of a subject consistent with the limits set forth in this General Order.

Definitions

Criminal Justice Information System (CJIS): A computerized system of criminal justice information, available twenty-four (24) hours a day and managed by the Commonwealth's Criminal History Systems Board.

Identification Document: An article/credential that is, or purports to be, issued by a government entity, that is relied upon to record or prove the identity of its bearer. Examples may include:

- A driver's license from any state or country;
- An ICE- issued identity/status card;
- A document issued by the Massachusetts Registry of Motor Vehicles (RMV), or other official governmental motor vehicle organization; and
- A passport issued by the U.S. State Department or any other sovereign nation.

Seizure: To take possession under compulsion of legal authority; to confiscate.

U.S. Immigration and Customs Enforcement (ICE): An agency within the Department of Homeland Security (DHS), its mission is to enforce the nation's immigration and customs laws.

Seizing Documents

Identification Documents may be seized from an individual only if they are:

- Contraband (including stolen, forged, or altered documents);
- The fruits or instrumentalities of a Massachusetts crime;
- Evidence of a Massachusetts crime; or
- Illegally possessed.

The seized documents shall be initially processed as required under INV-10 *Evidence Collection and Preservation*. Once the case is adjudicated, seized documents shall be promptly disposed of according to Department Policy and Procedure INV-11A *Property and Contraband*. Stolen passports seized for these purposes should initially be processed like any other evidence according to INV-10 & INV-11A. Once the case is adjudicated, passports should be forwarded to the originally intended holder, or the U.S. Department of State, Passport Services, **Consular Lost/Stolen Passport Section,** 1111 19th St. NW, Room 500, Washington, DC 20036.

State Residency

Foreign operators may drive in Massachusetts for up to one (1) year with their foreign license if they are a visitor. An operator with an out-of-state license may drive in Massachusetts at any time, provided they do not establish residency within the Commonwealth. However, pursuant to G.L. c. 90, § 8, once a foreign operator or an out-of-state operator becomes a Massachusetts resident, he or she must immediately obtain a Massachusetts driver's license.

A member may question an operator about his/her employment, current residence, and/or tax status, when the member possesses a reasonable suspicion that a person operating on a foreign or out-of-state license has established residency in Massachusetts and the member requires the information to aid in determining if the operator is in compliance with Massachusetts law.

Out-of-State Licenses

An out-of-state license should not be seized by a member unless this document is:

- Contraband;
- A fruit or instrumentality of a crime;
- Evidence of a crime; or
- Illegally possessed.

Seized licenses shall be processed in accordance with INV-10 & INV-11A.

Determining License Status

To determine if the operator has been living in Massachusetts for longer than one year, the following checks may be performed to aid in determining an operator's current status:

- A motor vehicle violations history check (KQ);
- A criminal history check (BOP);
- Utilize the CJIS screen titled "INS" to learn when the operator entered the U.S.;
- A RMV check to determine if the operator has any license status within Commonwealth; or
- The issuance a RMV "A" or "X" number.

Note: Massachusetts RMV issues an "A" number to individuals who are unlicensed within the Commonwealth, but have received a Massachusetts motor vehicle citation; an "X" number is issued to individuals who are unlicensed within Massachusetts, but own a Massachusetts registered motor vehicle.

Foreign Licensed Operators

Massachusetts shall only honor valid licenses from countries identified within the current Massachusetts Driver's Manual "A" Appendices: *Parties to the Road Traffic Convention and the 1943 Inter-American Automotive Traffic Convention*.

This publication is available to all members via the Massachusetts Registry of Motor Vehicles web site under:
Forms & Manuals→ Driver's Manual→ Appendices "A".

International Driver's License/ Permit

An international driver's license/permit is simply a translation of an operator's foreign driver's license into English. This document is not required to operate a motor vehicle in Massachusetts.

The international license/permit is not a substitute for a person's actual driver's license issued by their country of origin. An operator who is licensed in another country is required to carry only their valid foreign driver's license.

ICE Detainers

Department members are NOT authorized to stop, arrest, and/or take an individual into custody based solely on an ICE detainer.

If an individual is in Department custody pursuant to an arrest on criminal charges or a warrant, or for any other reason, the existence of an ICE detainer for that individual does NOT grant members of the Department authority to detain the individual for any period longer than they would otherwise be held in Department custody.

ICE Detainers, continued

Member Responsibilities

When a Department member conducts a NCIC/DCJIS query of an individual who is **already** in Department custody pursuant to arrest on criminal charges or a warrant and determines that the individual is the subject of an ICE detainer as defined in 8 C.F.R. § 287, the member shall **immediately** notify the Troop Duty Officer.

Troop/Duty Officer Responsibilities

The Troop Duty Officer shall instruct a Troop Dispatcher to contact ICE at (802) 872-6020 to notify ICE that an individual in custody is the subject of an ICE detainer.

The Troop Duty Officer shall monitor the status of an individual with an ICE detainer until the individual is released, transferred, or taken into custody by ICE. If ICE fails to take custody of the individual prior to the time when the individual would otherwise be released or transferred from Department custody, the individual shall be immediately released or transferred from Department custody. All such actions/inactions, and the reasons for the same shall be recorded in the appropriate daily administrative journal and/or reports.

Request for Voluntary Notification of Release

In certain circumstances, ICE will request, by providing *Form I-247A ("Immigration Detainer – Notice of Action")* that the Department **notify** ICE before an individual is released or transferred from Department custody. After receiving *Form I-247A* from ICE, the Troop Duty Officer shall notify ICE of the individual's impending release as early as possible and shall document the notification in the appropriate daily administrative journal and/or reports. Upon receipt of Form I-247A, the Troop Duty Officer shall also 1) relay a copy of the detainer form to any other law enforcement agency (including a jail, regional lockup, or state court) to which custody of the individual is transferred, and 2) shall notify ICE in the event of the individual's death, hospitalization, or transfer to another institution. **Under no circumstances will an individual be detained beyond the time s/he would normally be released from Department custody on the basis of the Department's receipt of *Form I-247A*.**

Bail Magistrate, Court, and District Attorney Notifications

In circumstances where an individual is eligible for bail, members shall notify the Bail Magistrate that the individual is the subject of an ICE detainer.

ICE Detainers, continued

In circumstances where an individual is transferred into the custody of the court system, the officer transporting the individual shall notify the court, district attorney's office, and other appropriate law enforcement agencies of the existence of an ICE detainer. This notification shall be documented in the appropriate daily administrative journal and/or reports.

Mandated Consular Reporting

Agreements with certain countries mandate that they be notified when their nationals are confined or detained regardless of the national's request.

When foreign nationals are involved in an incident, members shall consult "Consular Notification and Access" provided by the U. S. State Department, which is available to all members via the State Department website at: http://travel.state.gov/consularnotification

Seizure Procedures

If this occurs…	Then…
The operator is arrested for operating under the influence (OUI) of alcohol and fails a breath test, or refuses a breath test.	• Process as specified by M.G.L.; and • Seize Massachusetts licenses if appropriate. **Note**: If the operator is from out-of-state and possesses an out-of-state license, do not seize the license.
The operator has a suspended or revoked Massachusetts Driver's License.	• Seize the driver's license; • Complete a RMV Form 21188 – *Report and Affidavit of an Operating After Suspension/Revocation Incident*; • Forward both the license and Form 21188 to the RMV; and If the suspended or revoked operator is operating a vehicle registered to them, seize the registration plates and forward the plates to the RMV with Form 21188.
The operator possesses/uses a forged/altered license or any official document from the Massachusetts RMV or from another country or state's department of motor vehicles.	• Seize the forged or altered documents; • Notify the State Police Compliance Unit of this violation by utilizing RMV Form #T21193 – *Affidavit of Person Obtaining License*; and • Process seized documents in accordance with INV-10 & INV-11A. Note: The operator may be charged with G.L. c. 90, §24B, c. 90, §28, or c. 267, §1- (forgery statute).

Seizure Procedures, continued

If this occurs…	Then…
An operator presents a license from a foreign country.	See "Foreign Licensed Operators" Section.
A passenger in a vehicle presents a suspended or revoked Massachusetts license for identification purposes only.	• If the suspension/revocation is for OUI alcohol, seize the license and forward it to the RMV or destroy it; **however**, • If used for identification purposes only, the suspended/revoked license should not be seized.
The operator presents an out-of-state license, which is suspended, revoked, or expired in the operator's home state.	• Do not seize the license; • The operator may be charged with MGL Ch. 90, §10, unlicensed operation of a motor vehicle; and • Obtain the CJIS printout from the operator's home state to verify the suspension or revocation for court purposes.

References**:**

INV-10 Evidence Collection and Preservation;
INV-11A Property and Contraband;
Form I-247A Immigration Detainer – Notice of Action;
U.S. Department of State Publication; "Consular Notification and Access";
8 C.F.R. § 287;
Massachusetts Driver's Manual "A" Appendices: Parties to the Road Traffic Convention and the 1943 Inter-American Automotive Traffic Convention;
RMV Form 21188 – Report and Affidavit of an Operating After Suspension/Revocation Incident;
RMV Form #T21193 – Affidavit of Person Obtaining License.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**INV-18**
Subject:	
Mobile Identification Device Use	

Policy

This policy provides guidelines for the issuance, training, and use of Mobile Identification Devices.

Authorized and trained Members may access the Department's Automated Fingerprint Identification System and the Next Generation Identification system by the State Identification Section (SIS) for the use of Mobile Identification Devices to assist in the identification of individuals under appropriate circumstances and to provide for additional officer safety and situational awareness.

Definitions

Automated Fingerprint Identification System (AFIS): The computerized biometric matching system that stores identifying biometric templates and related demographics. The State AFIS maintains the following biometric information: known fingerprints and palm prints, latent fingerprints and palm prints, booking and tattoo photos, and iris images. SIS operates AFIS.

Biometrics: Distinctive, measurable physiological characteristics used to identify individuals. Commonly collected biometrics include fingerprints, palm prints, photographs (mug shots) and iris images.

Mobile Identification (ID) Device: A handheld scanning device that captures fingerprint images and utilizes a secure connection to submit them for search of selected fingerprint databases.

Mobile ID "HIT": Information returned from the Mobile ID search that an individual has been fingerprinted and/or that a highly probable matching record exists as indicated by a SID/CID from the state and/or a UCN from the FBI/NGI database(s).

> Note: Information returned from the Mobile ID search shall be confirmed by additional means subsequent to an arrest within a reasonable period of time. (e.g., confirmed by submitting booking fingerprints per DET-05 subsequent to an arrest).

NGI (Next Generation Identification): A biometric matching system operated by the FBI that creates a national electronic repository of biometric and criminal history information. Details on NGI can be found at: www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi

Definitions, continued

Repository for Individuals of Special Concern (RISC): A rapid search accessible to authorized law enforcement officers, available through a mobile fingerprint device. This search capability provides additional officer safety and situational awareness by providing access to the national repository of wants and warrants including Immigration Violator File (IVF) of the National Crime Information Center (NCIC), convicted sex offenders and known or appropriately suspected terrorists. This search is available only to authorized criminal justice personnel for criminal justice purposes in compliance with state and federal laws.

State Identification Number (SID) / Civil Identification Number (CID): A unique number associated with an individual's state fingerprint-supported identity. The SID is associated with a criminal identity and the CID is associated with civil identity.

Universal Control Number (UCN): A unique number associated with an individual's national fingerprint-supported identity. The UCN, formerly referred to as an FBI number, may be associated with either criminal or civil fingerprint records.

Issuance of a Mobile ID Device and Training

Department Members authorized to use Mobile ID Devices shall:

- Complete a Department-approved training course that includes:
  - Training based on manufacturer's recommendations and suggestions from the device vendor, or SIS;
  - Training on set-up, maintenance procedures, proper use guidelines, reporting requirements, and understanding of results.
- Demonstrate proficiency on the device operation;
- Ensure the issued devices are properly maintained in accordance with the manufacturer's recommendations; and
- Discontinue the use of any malfunctioning device and:
  - Notify their immediate supervisor, and SIS;
  - Ensure a malfunctioning device is returned to the device vendor, SIS or other designated entity for repair, as determined by SIS.

Subject:	Number:
Mobile Identification Device Use	**INV-18**

Use of a Mobile ID Device

Mobile ID Devices provide Department Members with the ability to obtain identification information or confirm the identity and criminal history of an individual. A Department Member may use a Mobile ID device when the individual ***consents***; and

- There is reasonable suspicion the individual has committed a crime; or
- The use of a scan will establish or nullify the individual's identity as the subject of an arrest warrant; or
- The individual provided a false or fictitious name, residential address, date of birth or other identifying information; and/or
- For officer safety and situational awareness.

Department Members shall be aware that:

- When consent is given, the individual may limit or withdraw consent at any time. The use of the Mobile ID Device is **no longer authorized** and must stop immediately once consent is withdrawn; and
- A member shall not coerce a subject to submit to the use of the Mobile ID Device.

The use of Mobile ID Device without the consent of an individual is permitted under specific circumstances which include, but are not limited to, the following:

- Subsequent to arrest or probable cause to arrest an individual;
- Pursuant to a valid court order;
- When specifically required by statute;
- When authorized by Department Standard Operating Procedure (SOP) or Policy and Procedure;
- During a medical emergency where the individual is unable to provide consent and identification; or
- The identification of a deceased individual.

The use of a Mobile ID Device shall:

- Be used to check the individual's fingerprint(s) against the existing database; and
- Not replace traditional booking fingerprinting procedures, however it may be used prior to traditional booking or fingerprinting procedures.

Subject:	Number:
Mobile Identification Device Use	**INV-18**

Prohibited Use of Mobile ID Devices

Mobile ID Devices assigned to Department Members shall not:

- Be used for random or generalized investigative or intelligence gathering;
- Be used without consent, or other legal justification;
- Be used for prohibited profiling, unlawful detentions, or unlawful searches; and
- Be used for inquiring about a person's immigration status, consistent with INV-17, for the sole purpose of facilitating that person's detention or deportation by U.S. Immigration and Customs Enforcement (ICE).

Responsibility

Department Members shall:

- Document within the investigative reports the specific circumstances relied upon for using the Mobile ID Device based on training, SOP, and policy as verification that an arrest was justified and appropriate; and
- Ensure any identification is confirmed by additional means that shall be documented in the investigative report.

References

DET-05 Identification of Persons in Department Custody;
INV-17 Travel/Immigration Status Inquiries & Investigations.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
December 6, 2021	**INV-19**
Subject:	
Use of Facial Recognition Technology	

General

Facial recognition technology involves the ability to examine and compare distinguishing characteristics of a human face through the use of biometric algorithms contained within a software application. This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce fraud, prevent individuals from becoming victims of identity theft, reduce an imminent threat to health or public safety, and help in the identification of persons unable to identify themselves or deceased persons.

The Department has access to the Massachusetts Registry of Motor Vehicles (MA-RMV) facial recognition system via a memorandum of agreement to support the investigative efforts of law enforcement within and outside the Commonwealth of Massachusetts. The Department does not authorize the use of any other facial recognition technology. The use of other facial recognition technology is prohibited without prior approval from the Office of the Superintendent.

Purpose

The purpose of this policy is to provide Department personnel with guidelines and principles related to utilization of the MA-RMV facial recognition system. The requirements imposed by this policy are in addition to any policies, procedures, requirements, restrictions, or directives imposed by the MA-RMV related to utilization of their facial recognition system. All utilization of the MA-RMV facial recognition system is for official use only.

Definitions

Biometric Data: Computerized data relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of such person, including, but not limited to, facial recognition, fingerprints, palm veins, deoxyribonucleic acid, palm prints, hand geometry or iris recognition.

Biometric Surveillance System: Any computer software that performs facial recognition or other remote biometric recognition.

Facial Recognition: An automated or semi-automated process that assists in identifying or verifying an individual or capturing information about an individual based on the physical characteristics of an individual's face, head or body, that uses characteristics of an individual's face, head or body to infer emotion, associations, activities or the location of an individual; provided, however, that "facial recognition" shall not include the use of search terms to sort images in a database.

Subject: Use of Facial Recognition Technology	Number: INV-19

Definitions, continued

Facial Recognition Search: A computer search using facial recognition to attempt to identify an unidentified person by comparing an image containing the face of the unidentified person to a set of images of identified persons; provided, however, that a set of images shall not include moving images or video data.

Facial Recognition Software: A category of biometric software that maps an individual's facial features mathematically and stores the data as a faceprint.

Match: For the purposes of this policy only, situations where investigative follow up has determined that probable cause exists to believe that two photos are in fact one in the same person.

Applicability

These guidelines apply to the Department's use of the MA-RMV facial recognition system.

These guidelines do not apply to the Department's acquisition, possession, and use of personal electronic devices, such as cell phones or tablets that utilize facial recognition technology for the sole purpose of user authentication.

These guidelines do not apply to the Department's acquisition, possession, and use of automated video or image redaction software; provided, that such software does not have the capability of performing facial recognition or other remote biometric recognition.

These guidelines do not limit the Department's ability to receive evidence related to the investigation of a crime derived from a biometric surveillance system; provided, that the use of a biometric surveillance system was not knowingly solicited by or obtained with the assistance of a public agency or any public official in violation of any section or subsection of this policy or relevant law.

Subject: Use of Facial Recognition Technology	Number: INV-19

Permitted Use

Any law enforcement agency requesting a facial recognition search within the MA-RMV Facial Recognition System shall only do so through a written request submitted to the Department. All requests received shall be forwarded to the Department's Fraud Identification Unit.

A law enforcement agency may request such a facial recognition search for the following purposes:

- To execute an order, issued by a court or justice authorized to issue warrants in criminal cases, based upon specific and articulable facts and reasonable inferences therefrom that provide reasonable grounds to believe that the information sought would be relevant and material to an ongoing criminal investigation or to mitigate a substantial risk of harm to any individual or group of people; or
- Without an order to identify a deceased person or if the law enforcement agency reasonably believes that an emergency involving substantial risk of harm to any individual or group of people requires the performance of a facial recognition search without delay. Any emergency request shall be narrowly tailored to address the emergency and shall document the factual basis for believing that an emergency requires the performance of a facial recognition search without delay.
- This subsection shall not apply to the department of state police when performing investigatory functions related to the issuance of identification documents by the registrar of motor vehicles.

Procedures for Use of MA-RMV Facial Recognition System

Only trained and authorized users assigned to the Department's Fraud Identification Unit may utilize the MA-RMV facial recognition system.

User names and passwords to the MA-RMV facial recognition system are not transferable, must not be shared, and must be kept confidential.

Fraud Identification Unit personnel who receive a request to utilize the MA-RMV facial recognition system must review the submitted photograph to determine its suitability for comparison purposes. Photographs that are not suitable will not be submitted for analysis via the MA-RMV facial recognition system and the requestor will be notified. The Department prohibits the use of facial recognition technology to analyze composite images.

Department personnel shall log all law enforcement requests for searches related to the MA-RMV facial recognition system in the appropriate Department database to include the following information:

- A copy of any written request made for a facial recognition search;
- A copy of any court order, if applicable;
- Date and time of the request;

Procedures for Use of MA-RMV Facial Recognition System, continued

- Number of matches returned, if any;
- The database searched;
- Name and position of the requesting individual and employing law enforcement agency;
- The reason for the request, including, but not limited to, any underlying suspected crime;
- The entity to which the request was submitted;
- Data detailing the individual characteristics included in the facial recognition request;
- Requester's case number, file number, or incident number;
- Such documentation shall not be a public record, except as provided by applicable state law; and
- The Department shall report such documentation quarterly to the Executive Office of Public Safety and Security (EOPSS).

Reporting to EOPSS

The Department shall document each facial recognition search performed and shall provide such documentation quarterly to the Executive Office of Public Safety and Security.

Such documentation shall include:

- A copy of any written request made for a facial recognition search;
- The date and time of the request;
- The number of matches returned, if any;
- The database searched;
- The name and position of the requesting individual and employing law enforcement agency;
- The reason for the request, including, but not limited to, any underlying suspected crime;
- The entity to which the request was submitted; and
- Data detailing the individual characteristics included in the facial recognition request.

Reservations

These guidelines are set forth solely for the purpose of internal Department guidance. They are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter, civil or criminal, nor do they place any limitation on otherwise lawful investigative and legal prerogatives of the Massachusetts State Police, or the Commonwealth of Massachusetts.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
June 29, 2023	**INV-20**
Subject:	
Covert Audio Recordings	

Policy

Investigations utilizing covert surveillance/recording technology shall be conducted in accordance with applicable federal and state laws and regulations, and Department policy.

Authorized covert recordings shall only be made by trained Department members utilizing Department approved technology.

The use of monitoring technology for the purposes of officer safety, that does not generate any recorded or discoverable data is allowed. Members must familiarize themselves with all capabilities of the technology to ensure adherence to this policy.

The Department shall maintain records related to what covert recording technologies are approved for use and which members have been trained and authorized to use covert recording technology.

Definitions

Covert Audio Recording – An audio recording of the voice of one or more individuals without their knowledge or consent. This includes any video recording made in conjunction with an audio recording.

Non-Consensual Recording – A covert audio recording that is made without the knowledge and consent of any party to the conversation. *A wiretap warrant is required to make non-consensual recordings in all circumstances.*

One-Party Consensual Recording – A covert audio recording that is made with the knowledge and consent of at least one party, but not all parties, to a conversation.

All-Party Consensual Recording – An audio recording, commonly referred to as a two-party consensual recording, that is made with the knowledge of all participants in the conversation that is being recorded. All-party consensual recordings are <u>not</u> considered to be covert audio recordings and are not further contemplated in this policy. When made during the course of a criminal investigation, all-party consensual recordings shall be considered evidence, preserved in accordance with state records retention laws, and only deleted pursuant to the provisions of 19-SM-03 Procedures for Disposition of Evidence, Contraband, and/or Controlled Substances.

Covert Audio Recordings

Covert audio recording during the course of a criminal investigation is prohibited without documented supervisory approval.

Members seeking to utilize covert audio recording methods of any kind shall:

- Successfully complete any training on the covert recording technology that is required by their Division Commander prior to the use of the technology in a criminal investigation.
- Possess a full understanding of the capabilities of the covert recording technology to be employed prior to using the technology in a criminal investigation.
- Not initiate any covert recording prior to obtaining supervisory approval unless exigent circumstances exist. If initiation without prior approval is undertaken the recording member shall document the circumstances in a written report to be filed with their immediate supervisor upon expiration of said exigency.
- Indicate the intended use of covert recordings in operations plans.
- Obtain written authorization, when applicable, from a Supervisory Special Agent or Assistant United States Attorney, for use of Department equipment to make one-party consensual recordings in federal investigations.
- Prior to making any one-party consensual recordings in state investigations, either obtain a warrant pursuant to Commonwealth v. Blood 400 Mass. 61 (1987) or confirm that the prosecuting agency of jurisdiction does not believe that a warrant is legally required to make the intended recordings.
- Not utilize personal devices to create or store recordings of covert operations.
- Adhere to relevant federal law as well as the policy and procedures of the lead federal law enforcement agency when seeking to make one-party consensual recordings in a federal investigation.
- Secure a wiretap warrant when seeking to make non-consensual recordings in either state or federal investigations pursuant to Massachusetts General Laws c.272§ 99 and/or the Title III of The Omnibus Crime Control and Safe Streets Act of 1968.
- Document the existence and supervisory approval of all covert recording(s) within a written investigative report.
- Adhere to the notification requirements of ADM-16 Notifying Prosecuting Agencies Regarding Evidence with all covert audio recordings.

Creating a Clear and Complete Record

In order to ensure that the circumstances surrounding every covert recording are clear and fully documented, members shall:

- Not share covert recording accounts that are electronically assigned to specific members, since this can give the impression that the covert recording was made by the account holder rather than the member who actually made the recording. (This does not apply to covert recording technology that is intended to be shared and that does not save recordings in a virtual file/account assigned to a specific member.)
- Verify that the correct time is displayed on covert recording technology that imprints the date and time on the recording or in the metadata of the recording.
- Whenever practicable, record a preamble at the beginning of every covert recording that clearly indicates the date, time, location, name of the officer making or supervising the recording, code name of any confidential informant making or participating in the recording, and the case number for which the recording is being made.
- Document the date, time, location, name of the officer making or supervising the recording, code name of any confidential informant making or participating in the recording, and the case number for which the recording is being made within a written investigative report.
- Label the covert recording digital file that is created with the case number and a brief description of the event captured on the recording (e.g. 2023-000-0000 UC Buy from John Doe in Fitchburg 5-25-23 @ 0000 hrs.).

Supervisory Responsibilities

Supervisors receiving requests from personnel seeking to employ the use of covert recordings during an investigation shall:

- Confirm the technology is appropriate for the investigation; and
- Ensure the technology to be used has been approved by their Division Commander.
- Confirm personnel who will utilize the covert recording equipment are fully aware of its capabilities and have successfully completed any training on the technology that has been mandated by their Division Commander.
- Conduct ongoing reviews of covert recordings for adherence to applicable federal and state laws and regulations, and Department policy.

Subject:	Number:
Covert Audio Recordings	**INV-20**

Preservation and Storage

- Covert recordings shall be considered evidence, preserved in accordance with state records retention laws, and only deleted/destroyed pursuant to the provisions of 19-SM-03 Procedures for Disposition of Evidence, Contraband, and/or Controlled Substances.

- Whenever possible, an exact copy of the original recording shall be attached to an ACISS report in the ACISS case for which the recording was made. Uploading an exact copy of an original recording into ACISS in this fashion shall satisfy this provision to preserve the recording as evidence.

- In circumstances where it is not possible to upload an exact copy of the original recording into ACISS, members shall upload an exact copy of the original recording to a stable digital storage medium (e.g. hard drive, USB Drive, or CD/DVD) and enter this stable digital storage medium into evidence at an involved station/section/unit in accordance with INV-11A Evidence/Contraband/Property Intake-Storage.

- Pursuant to INV-01A Case Management, the assigned Case Officer is responsible for accounting for all the evidence in a case, including all covert recordings. The Case Officer is also responsible for coordinating with the prosecutorial authority to ensure that discovery obligations are met. Additionally, the production of all discovery to prosecuting agencies shall be documented in a Department report that is maintained within the case file.

References:

ADM-16;
INV-01;
INV-01A;
INV-10;
19-SM-03;
23-SM-03;
Massachusetts General Laws c.272§ 99;
Commonwealth v. Blood, 400 Mass 61 (1987)
Commonwealth v. Mora, 485 Mass 360 (2020);
Commonwealth v. Rainey, 491 Mass 632 (2023).
Title III of The Omnibus Crime Control and Safe Streets Act of 1968

Promulgated By: John E. Mawn Jr, Colonel/Superintendent

Massachusetts State Police
Policy and Procedure
Index

ADMINISTRATIVE

CODE	TITLE	DATE
ADM-01	Oath of Office	5/25/2023
ADM-02	State Police Mission and Policy	5/25/2023
ADM-04	State Police Authority	5/25/2023
ADM-05	Organizational Structure	5/25/2023
ADM-06	Command Staff Responsibilities	5/25/2023
ADM-07	Written Directives, Schedules and Forms	11/10/2021
ADM-08	Strategic Planning	7/22/2022
ADM-08A	Grant Approval Process	7/22/2022
ADM-09	Line Inspections	7/22/2022
ADM-09A	Staff Inspections	7/22/2022
ADM-10	Awards	5/25/2023
ADM-11	Sick Leave	11/10/2021
ADM-11A	Temporary Modified Duty	11/10/2021
ADM-11B	Injury Reporting and Leave	11/10/2021
ADM-11C	Maternity Leave and Guidelines	5/25/2023
ADM-11E	Leaves of Absence	5/25/2023
ADM-12	Serious Injury/Death of a Member	7/22/2022
ADM-13	Notification of Medical Examiner and/or Next of Kin	7/22/2022
ADM-14	Personnel Investigations	5/25/2023
ADM-15	Internal Affairs Investigations	5/25/2023
ADM-16	Notifying Prosecuting Agencies Regarding Evidence	7/22/2022
ADM-17	Employee Evaluation System	5/25/2023
ADM-18	Unlawful Harassment, Sexual Harassment and Discrimination	11/10/2021
ADM-19	Vehicle Management	5/25/2023
ADM-19A	Vehicle Use and Maintenance	5/25/2023
ADM-19B	Automated Vehicle Locator (AVL) Technology	5/25/2023
ADM-20	Weapons Management	11/10/2021
ADM-21	Communications	5/25/2023
ADM-22	Court Attendance and Fees	7/22/2022
ADM-24	Department Radio Call Signs	5/25/2023
ADM-25	Paid Details	2/21/2023
ADM-26	Military Service	5/25/2023
ADM-27	Transfers	12/6/2022
ADM-28	Department Motor Vehicles	7/22/2022
ADM-29	Workplace Violence	7/22/2022
ADM-30	Asset Management	5/25/2023
ADM-34	Information Technology Resources (ITR)	5/25/2023

ADM-34A	Social Media/Networking	5/25/2023
ADM-35	Body-Worn and Cruiser-Mounted Cameras	11/10/2021
ADM-36	Diversity and Equal Opportunity	11/10/2021
ADM-41	Telephone Use/Access	5/25/2023
ADM-46	Sexual Activity in Public Places	7/22/2022
ADM-47	Bias-Based Policing	5/25/2023
ADM-49	Deaf or Hard of Hearing Individuals	5/25/2023

DETAINEE

CODE	TITLE	DATE
DET-01	Warrant Management	11/10/2021
DET-01A	Warrants, Summons, or Subpoenas	11/10/2021
DET -02	Custodial Inventory	11/10/2021
DET -03	Detainee Transportation	11/10/2021
DET -04	Holding Facility Design and Inspection	11/10/2021
DET -05	Identification of Persons in Department Custody	11/10/2021
DET -06	Detainee Monitoring	11/10/2021
DET -07	Detainee Sexual Abuse and Sexual Harassment	11/10/2021
DET -07A	Detainee Sexual Abuse and Sexual Harassment Investigations, Review and Data Collection	11/10/2021
DET -08	Gender Identity and Expression	11/10/2021
DET -09	Juvenile Operations	12/6/2021
DET -10	Protective Custody	11/10/2021

GENERAL

CODE	TITLE	DATE
GEN-01	Personal Appearance	5/25/2023
GEN-01A	Tattoos and Body Modifications	5/25/2023
GEN-02	Uniforms	5/25/2023
GEN-04	Military Courtesy	7/22/2022
GEN-04A	Ceremonial Tributes	7/22/2022
GEN-05	Communicable Diseases	5/25/2023
GEN-06	Drug Testing	5/25/2023
GEN-07	Automatic External Defibrillators	11/10/2021
GEN-08	Ride-Along/Observer	11/10/2021

INVESTIGATIVE

CODE	TITLE	DATE
INV-01	Criminal Investigations	5/25/2023
INV-01A	Case Management	5/25/2023
INV-02	Confidential Informants	7/22/2022
INV-02A	Confidential Funds	11/10/2021
INV-03	Prescription Monitoring Program	5/25/2023
INV-05	Special Protections for Juveniles	11/10/2021
INV-07	Non-Published Telephone Numbers	5/25/2023
INV-08	Criminal Intelligence	11/10/2021
INV-09	Polygraph Examinations	5/25/2023

INV-10	Evidence Collection and Preservation	5/25/2023
INV-11	Controlled Substance-Storage & Handling	9/22/2022
INV-11A	Evidence/Contraband/Property Intake-Storage	5/25/2023
INV-13	Asset Forfeiture	5/25/2023
INV-14	Seized Currency	5/25/2023
INV-15	Field Interview and Observation Reports	11/10/2021
INV-16	Electronic Recording of Interrogations	7/22/2022
INV-16A	Eyewitness Identification	5/25/2023
INV-17	Travel/Immigration Status Inquiries & Investigations	7/22/2022
INV-18	Mobile Indentification Device Use	7/22/2022
INV-19	Use of Facial Recognition Technology	12/6/2021

SPECIAL OCCURRENCES

CODE	TITLE	DATE
SOC-01	Hazardous Materials	5/25/2023
SOC-02	Bomb Threats/Explosive Incidents	5/25/2023
SOC-03	Emergency Planning	5/25/2023
SOC-03A	Emergency Operations Center (EOC)	11/10/2021
SOC-03B	Response to Emergency Situations	5/25/2023
SOC-03C	Response to Civil Disturbances	5/25/2023
SOC-03D	All Hazards Incident Command Framework	5/25/2023
SOC-03E	Emergency and Continuity Plan Requirements	5/25/2023
SOC-04	Lost/Missing Person Searches	5/25/2023
SOC-04A	Amber Alert Activation	5/25/2023
SOC-05	Special Considerations	7/22/2022
SOC-06	Administration of Naloxone Hydrochloride (Narcan)	7/22/2022
SOC-07	Domestic Abuse	7/22/2022
SOC-07A	Domestic Abuse Arrest/Investigations	5/25/2023
SOC-07B	Domestic Abuse Involving Members	7/22/2022
SOC-07C	Abuse of Children/Disabled/Elderly	7/22/2022
SOC-08	Missing/Abandoned/Runaway Children	7/22/2022
SOC-09	Terrorism/ WMD Incidents	7/22/2022
SOC-10	Clandestine Drug Laboratory Response	7/22/2022

SUPPORT

CODE	TITLE	DATE
SUP-01	Jurisdiction/Mutual Aid	5/25/2023
SUP-03	Media Relations	5/25/2023
SUP-04	Employee Assistance Unit	11/10/2021
SUP-04A	Critical Incident Stress Management Team	2/17/2023
SUP-05	State Police Chaplain Corps	5/25/2023
SUP-06	Binding Written Agreements	7/22/2022
SUP-12	Office of the Ombudsman	7/22/2022

TACTICAL OPERATIONS

CODE	TITLE	DATE
TOP-01	Special Operations Command and Control	5/25/2023
TOP-02	Special Tactical Operations Team	5/25/2023
TOP-03	Crisis Negotiation Team	5/25/2023
TOP-04	Mounted Unit	5/25/2023
TOP-05	Canine Unit	5/25/2023
TOP-06	Underwater Recovery Team	5/25/2023
TOP-07	Air Wing	5/25/2023
TOP-07A	Small Unmanned Aerial System (UAS)	5/25/2023
TOP-08	Marine Unit	7/22/2022
TOP-09	Incident Management Assistance Team	5/25/2023
TOP-10	Special Emergency Response Team	7/22/2022
TOP-11	Emergency Management Unit	7/22/2022
TOP-12	Motorcycle Unit	7/22/2022
TOP-13	Behavioral Observation and Suspicous Activity Recogition Unit (BOSAR)	5/25/2023

TRAFFIC

CODE	TITLE	DATE
TRF-01	Mission, Goals, and Objectives	5/25/2023
TRF-02	Patrol	11/10/2021
TRF-03	Selective Traffic Enforcement	5/25/2023
TRF-04	Motor Vehicle Pursuits	12/6/2021
TRF-04A	Foot Pursuits	5/25/2023
TRF-05	Traffic Incident Management	5/25/2023
TRF-07	Motor Vehicle Stops	11/10/2021
TRF-08	Citations	11/10/2021
TRF-09	Towing	7/22/2022
TRF-10	Vehicle Inventory	7/22/2022
TRF-11	Automatic License Plate Recognition	11/10/2021
TRF-12	Crash Investigations	11/10/2021
TRF-14	Operating Under the Influence-Alcohol	5/25/2023
TRF-14B	Preliminary/Portable Breath Test Devices	5/25/2023
TRF-15	Sobriety Checkpoints	5/25/2023
TRF-16	Speed Measuring Devices	5/25/2023
TRF-17	Emergency Roadblocks	7/22/2022
TRF-20	Department Vehicle Crashes	5/25/2023
TRF-21	Tire Deflation Devices	7/22/2022
TRF-22	Escorts and Relays	7/22/2022

TRAINING

CODE	TITLE	DATE
TRN-01	Training Administration	5/25/2023
TRN-02	Recruit Training	5/25/2023
TRN-03	Field Training Program	5/25/2023
TRN-04	Professional Development	5/25/2023

TRN-05	State Police Cadet Program	11/22/2022

USE OF FORCE

CODE	TITLE	DATE
UOF-01	Use of Force	5/25/2023
UOF-02	Lethal Force-Response	5/25/2023
UOF-03	Reports	5/25/2023
UOF-04	Use of Force-Equipment	5/25/2023
UOF-05	Firearms Qualification	5/25/2023
UOF-06	Electronic Weapons Control (ECW)	5/25/2023

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**SOC-01**
Subject:	
Hazardous Materials	

Policy

Department personnel, unless properly equipped and trained, shall not be deployed into areas that have been contaminated or face an immediate and substantial threat of contamination with a hazardous material.

Hazardous material response training shall be provided to trainees during the Recruit Training Troop and subsequently to veteran Department members through annual awareness training.

Definition

Hazardous Materials: Chemicals, biological agents or organisms, or radiological substances that are damaging to health or property.

Responding Members

If…	Then members shall…
There is no known or potential presence of a hazardous material on scene; or There is a hazardous material on scene, but it is properly secured and poses no threat of release:	• Respond with due caution; and • Ensure that the Emergency Response Guidebook is accessible.
It is possible to ascertain from a safe distance the identity of a substance or cargo via use of placards or other identification:	• Relay information to the Desk Officer; and • Consult the Emergency Response Guidebook.
There is an immediate and substantial threat of the release of a hazardous material on scene:	• Consult the Emergency Response Guidebook for guidance as to maintaining a safe distance from the area of possible contamination.
Dangerous conditions are observed:	• Take immediate action to ensure their own safety, the safety of other responding officers or personnel, and the safety of the general public; and • Communicate the nature of the threat to the Desk Officer.

Desk Officer

Upon receiving a report of an incident that may involve a hazardous material, the Desk Officer shall make every reasonable effort to obtain available information from the scene.

The following information shall be obtained and relayed to responding members and to the Troop Duty Officer:

- The type of container/vehicle;
- Whether the container/vehicle is leaking;
- Department of Transportation (DOT) placards, labels or numbers;
- Carrier name and any information found in shipping papers;
- Local area road and weather conditions; and
- Other responding resources and/or agencies.

Upon receiving a report of an incident that may involve a hazardous material, the Desk Officer shall notify:

- Assigned patrol and other members in the area;
- Troop Duty Officer;
- Local police department;
- Local fire department; and
- Department of Fire Services-Regional Hazardous Materials Team: (877) 385-0822.

Desk Officer-Actual Release or Threat of Release

On receiving a report of an incident involving the actual release or threat of release of a hazardous material, the Desk Officer shall:

- Immediately notify the Troop Duty Officer;
- Notify available resources to include: local fire department, Department of Fire Services-Regional Hazardous Materials Team, Commercial Vehicle Enforcement Section, for initial emergency hazmat actions;
- Obtain expertise from the Emergency Response Guidebook regarding:
  - Scope of contamination; and
  - Minimum safe evacuation zone for unprotected individuals prior to deploying Department personnel; and
- Notify the Massachusetts Department of Environmental Protection at (888) 304-1133 and provide the following information:
  - Location;
  - Type and quantity of material released;
  - Suspected impacts if known (catch basin, wetlands);
  - Name, address, and phone number of carrier (if known);
  - Special conditions which responders should be aware of to facilitate the safe mitigation of the release; and
  - Any other information which may be helpful.

Troop Duty Officer

The Troop Duty Officer shall:

- Dispatch a supervisor to the scene;
- Notify the Troop Commander;
- Notify GHQ Communications at (508) 820-2121; and
- When applicable, notify the Commercial Vehicle Enforcement Section at (978) 369-1004, or if after hours, GHQ Communications at (508) 820-2121.

Patrol Supervisor

Supervisors shall establish an outer perimeter, referencing the Emergency Response Guidebook and available expertise to determine an appropriate distance from the incident.

Supervisors shall:

- Ensure that Department personnel are not deployed contrary to the provisions of this policy;
- Establish a command post upwind and uphill (if possible) and at a sufficient distance from the hazard; and
- Follow incident command procedures.

GHQ Communica-tions

If radioactive material is involved, the GHQ Communications Section shall notify the Department of Public Health Director of Radiation Control Program (617) 242-3055.

If no determination has been made as to who spilled the hazardous material, the GHQ Communications Section OIC shall notify the National Response Center (NRC) at (800) 424-8802.

Hazardous Materials Team

The head of the local fire department or designee shall activate the Department of Fire Services-Regional Hazardous Materials Team.

Available Official Expertise

The following are resources for information on hazardous materials:

- State expertise:
  - Department of Fire Services-Regional Hazardous Materials Team at (877) 385-0822;
  - Massachusetts Department of Environmental Protection at (888) 304-1133;
  - Department of Public Health Director of Radiation Control Program (617) 242-3055;
  - Bomb Squad; and
  - Commercial Vehicle Enforcement Section.

Subject:	Number:
Hazardous Materials	**SOC-01**

Available Official Expertise, continued

- Federal expertise:
  - CHEMTREC at (800) 424-9300; and
  - The National Response Center at (800) 424-8802 provides emergency chemical/biological assistance twenty-four (24) hours a day.

- Additional resources:
  - Querying MQ in the task field of the CJIS computer, and entering the placard information; and
  - Consulting the Emergency Response Guidebook.

References:
29 CFR 1910.120;
40 CFR 311.1;
527 CMR Section 1.03 (8);
U.S. Department of Transportation Emergency Response Guidebook;
Criminal Justice Information System (CJIS);
MPAC: 46.3.4.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**SOC-02**
Subject:	
Bomb Threats/Explosive Incidents	

Policy

The Bomb Squad is tasked with rendering safe any explosive (e.g., Improvised Explosive Device (IED), military or commercial explosives) within the Commonwealth of Massachusetts. The Fire and Explosion Investigation Unit (FEIU) Commander or designee is responsible for determining a response to any bomb threat.

The Department shall:

- Maintain and support a Bomb Squad comprised of members with specialized training, expertise, and equipment to include explosive detection K-9s.

The Bomb Squad shall:

- When assigned, assist officers from the Department and from other local, state, federal and military agencies to deal with potential life threatening explosive related incidents, chemical, biological, radiological and nuclear (CBRN) incidents as well as clandestine drug lab activity;
- Train first responders in explosives and IED recognition; and develop, under the direction of the Section Commander, a unit specific Standard Operating Procedure (SOP) which shall be maintained and updated as necessary.

Purpose

- To establish and define the role of the Bomb Squad within the Division of Investigative Services - Fire and Explosion Investigation Unit (FEIU), and to establish guidelines for utilization and activation of their members.

Response Guidelines

Since the validity of a bomb threat cannot be determined initially, the decision to evacuate or to re-occupy the threatened premises is the responsibility of the owner or manager of the premises or the head of the fire department or designee.

Department members shall not order an evacuation based only on a threat. If advice is sought from the Department, the recommendation should be to follow the Massachusetts Bomb Threat Response Guidance.

If a suspected explosive device or suspicious package has been located or if there is a perceived threat, the head of the fire department or designee has the authority to order an evacuation under MGL c.148.

Utilization of Bomb Squad

Bomb Squad Team members are available twenty-four (24) hours a day for:

- Rendering safe any explosive (e.g., IED, military or commercial explosives);
- Security sweeps for high profile events and visiting dignitaries;
- Response and technical assistance/advice for bomb threats;
- Weapons searches with Explosive K-9s;
- Homeland Security assignments;
- Retrieval and remediation of energetic materials to include ammunition, fireworks, gun powder, etc.; and
- Other special events/incidents as assigned.

Emergency Activation Protocol

Requests for the Bomb Squad shall be made to the Troop Duty Officer and shall include:

- Date and time of request;
- The name, rank, and agency name of the requesting officer;
- The name of the primary point of contact and a direct call-back number;
- The nature of the request;
- Primary and secondary Department members dispatched; and
- The exact location of the incident and any designated staging areas.

The Troop Duty Officer shall make appropriate Daily Administrative Journal entries.

Activation/ Contact

Type of Request	Contact
Emergency	• Troop Duty Office of jurisdiction.
Non-emergency	• During business hours contact the FEIU at 978-567-3310. • After business hours contact the Troop Duty Office of jurisdiction.

Authority

Any officer who encounters or seizes any bomb or other high explosive is required under MGL Chapter 266, § 102D(a) to make immediate notification to the State Fire Marshal. Bomb Squad members shall assume complete control and authority of any explosives render-safe procedure under Incident Command System (ICS) protocols.

While at an active scene, command and control of the scene shall be exercised only by:

- Bomb Squad Commander or designee;
- FEIU Commander or designee;
- Unified Commanders on scene (ICS);
- Division of Investigative Services Commander or designee; or
- Superintendent/Deputy Superintendent.

Response Protocols

All Department members shall take appropriate measures to ensure the safety of people and property while awaiting the arrival of the Bomb Squad.

The first on-scene or investigating member shall assess the situation and determine the need for additional resources including, but not limited to:

- Local Police/Fire Department(s) as well as additional Department resources to include: Crime Scene Services, State Police Detective Unit of jurisdiction, Commonwealth Fusion Center;
- Emergency Medical Services (EMS); and
- Traffic control.

To reduce the risk of detonation, members responding to an explosives threat or incident shall NOT:

- TOUCH, MOVE or DISTURB any suspicious objects, items or packages;
- Allow anyone within three-hundred (300) feet of a suspicious device;
- Allow anyone to be in the path of possible shrapnel or flying glass;
- Utilize electronic communication devices within close proximity to the unattended/suspected item; or
- Direct flashlight beams onto a possible device or use a camera flash (in order to prevent activation by photoelectric cell).

Never rule out the <u>possibility of a secondary or tertiary</u> device.

Responding members shall remain on the scene until properly relieved.

Evidence Considerations

Evidence and materials collection shall be coordinated by FEIU members. Evidence custody shall remain with the lead State Police case officer.

After Action Reporting

Following the completion of any critical incident, Bomb Squad members may be debriefed.

The Bomb Squad Commander or designee is responsible for the completion of any after action reports or Bomb Squad reporting as applicable. After Action Reports shall be forwarded to the Division of Investigative Services Commander for review.

Subject:	Number:
Bomb Threats/Explosive Incidents	**SOC-02**

References: Massachusetts Bomb Threat Response Guidance;
MGL Chapter 266, § 102D(a);
MGL c.148;
MPAC: 81.2.3.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Policy Date:	Number:
May 25, 2023	**SOC-03**
Subject:	
Emergency Planning	

Policy

The Department shall develop and implement an emergency operational response strategy to address potential public safety threat(s) or the actual occurrence(s) as identified in Homeland Security Presidential Directive 8 (HSPD-8).

Purpose

To maintain and ensure the Department's compliance with HSPD-8 with regards to emergency planning.

General Considerations

The Department must plan for foreseeable emergencies. Certain incidents require preplanning by Troop/Section Commanders within specific operational areas. Examples of these include:

- A general emergency that may result from a natural or man-made disaster, including civil disorder, acts of terrorism and / or other unusual occurrences;
- Disasters including floods, hurricanes, earthquakes, explosions, and tornadoes;
- Civil disorders including rioting and other acts of violence.
- Planning for special operations that require general emergency planning concepts; and
- Plans for application to site and situation specific circumstances when time allows, such as hostage or disturbances at correctional facilities.

Plans may be general initially and then become specific. In some circumstances, such as localized weather emergencies or dignitary protection details, certain information may not yet be known, but as much general information as possible should be preplanned with specifics inserted as the emergency occurs; emerging data or circumstances can be addressed as soon as they develop or can be predicted. Target areas and populations should be identified with equipment, personnel needs, the location of staging areas and emergency shelter locations identified beforehand.

General Considerations, continued

Planning for emergency operations promotes efficiency. Preplanning allows for immediate and decisive action that can minimize loss of life, reduce property damage and permit involved authorities to fulfill their responsibilities. Other efficiencies include:

- Emergency equipment can be acquired and readied for deployment;
- Personnel requirements can be more accurately predicted;
- Coordination procedures can be devised and tested;
- Different strategies and tactical options can be assessed;
- Contingency responses can be developed; and
- Durable intelligence information can be assessed before the emergency occurs.

General Plan Provisions

Emergency Plans should include the following provisions, as necessary:

- Communications;
- Situation Maps;
- Field Command Posts;
- Chain of Command (to include other agencies);
- Casualty information;
- Community Relations;
- Public Information;
- Rumor Control;
- Other Agency Support & Liaison;
- Military Support;
- Martial Law;
- Public Facility Security;
- Transportation;
- De-Mobilization Procedures;
- Court & Prosecutorial Liaison;
- Legal Authority;
- Post Occurrence (Aftermath) Duties; and
- After Action Incident Reports.

Responsibilities

Position	Duties
Colonel/ Superintendent	Shall: • Designate a Commissioned Officer as the Emergency Planning Officer; • Review and approve Emergency Operation Plans (EOPs) and Incident Action Plans (IAPs) submitted by the Emergency Planning Officer; and • Ensure that all EOPs written after October 2005 are National Incident Management System (NIMS) compliant.

Responsibilities, continued

Position	Duties
Emergency Planning Officer (EPO)	Shall: • Maintain all Department emergency response plans and standard operating procedures (SOPs) devised for nuclear facilities, prisons, natural or man-made disasters, and similar circumstances; and shall also retain copies of Troop emergency response plans devised for DOC facilities; • Study, draft and maintain appropriate contingency plans for foreseeable circumstances or events for which a Department response may be required; • Prepare EOPs and IAPs and submit them to the Colonel/Superintendent; • Coordinate the creation of EOPs and IAPs with Division Emergency Planning Coordinators; • Annually review and update the EOPs and IAPs; • Ensure that all EOPs written after October 2005 are NIMS compliant; • Coordinate Department contingency planning and liaison with the Massachusetts Emergency Management Agency (MEMA) and the Military Division of the Commonwealth; • Ensure plans for a Department response to terrorism and civil disorder are created and maintained; • Review Department emergency response plans at least annually and report the results of this review in a written report to the Division Commander of Homeland Security and Preparedness; and • Ensure the Department maintains a minimum of a 60 day supply of: Personal Protective Equipment (PPE), decontamination and cleaning products, and individual hand sanitizers, unless otherwise directed by the Colonel.

Responsibilities, continued

Position	Duties
Division Commanders	Shall: • Designate a Commissioned Officer as the Division Emergency Planning Coordinator; • Evaluate EOPs and IAPs through simulation exercises prepared by the Emergency Planning Officer; • Report deficiencies in EOPs and IAPs to the Emergency Planning Officer; and • Ensure that all EOPs written after October 2005 are NIMS compliant.
Troop/Section Commanders	Shall: • Designate a Commissioned or Non-Commissioned officer as the Troop/Section Emergency Planning Coordinator; • Evaluate EOPs and IAPs through simulation exercises prepared by the Emergency Planning Officer; • Report deficiencies through channels in EOPs and IAPs to the Emergency Planning Officer; and • Each Troop Commander shall develop, at a minimum, the framework of a plan to implement an initial response for the following types of incidents: o Natural or man-made disaster; o Civil disturbances and other unusual occurrences; o Hostage situations and barricaded persons; o VIP protection details; and o Other special events.
Troop/Section Emergency Planning Coordinator	Shall: • Assist the Division Emergency Planning Coordinator with the establishment of EOPs and IAPs; • Prepare and annually update, the Troop/Station/Section/Unit Emergency Planning Manual, EOPs and IAPs; and • Act as the liaison with the Division Emergency Planning Coordinator.

Emergency Planning Manual

The Department shall maintain and annually update an Emergency Planning Manual for the purpose of responding to and controlling hazardous situations through the prudent use of Departmental and external resources.

The Emergency Planning Manual shall be located at every State Police facility. It shall be updated annually, or as required.

The Manual shall include all current EOPs, IAPs, operational guidelines, on site operational instructions, personnel and equipment resource inventories and other necessary information, including but not limited to:

- Personnel and skills;
- State Police property and buildings;
- Supplies (food, fuel, clothing);
- Vehicles;
- Arrest/confinement procedures;
- Topographical maps;
- Support equipment;
- Incident Command Posts;
- Field Command Posts;
- Communications;
- Miscellaneous Equipment (generators, boats, etc.);
- Fleet vehicles;
- After action reporting;
- ICS Form 205;
- ICS Form 205A-OS;
- ICS Form 206; and
- Identified Staging Areas.

Drafting Emergency Plans

When drafting an emergency response plan or SOP:

- Describe all adverse elements;
- Use available intelligence summaries (Fusion Center); and
- Involve partner agencies with planning or operations, including but not limited to:

Local police departments;
Local fire departments;
MEMA;
Military Division of the Commonwealth;
MassDOT;
Massport;
Department of Corrections (DOC);
MA and Federal Courts;
Massachusetts Water Resources Authority(MWRA);
Department of Conservation and Recreation (DCR);
Mutual aid states (NESPAC);
Alcohol, Tobacco, and Firearms (ATF);
U.S. Secret Service;
Homeland Security;
Federal Bureau of Investigation (FBI);
National Transportation Safety Board (NTSB);
Federal Aeronautics Administration (FAA); and
U.S. Department of Defense.

Drafting Emergency Plans, continued

A plan should begin with a general assumption that an emergency will develop within the Commonwealth and:

- Normal procedures will not adequately protect life or property or preserve order; and
  - Will be beyond the capabilities of local authorities and shall require Department assistance; or
  - Will be beyond the capabilities of local authorities and the Department and may require National Guard or federal assistance to protect life and property and maintain order;

- That a national emergency may require the full resources of the Department to conduct emergency operations; and

- Immediate and decisive action is required to minimize loss of life, reduce property damage and permit involved authorities to fulfill their responsibilities.
  - Emergency equipment can be acquired and readied for deployment;
  - Personnel requirements can be more accurately predicted;
  - Intra-Department and interagency coordination procedures can be devised and tested;
  - Different strategies and tactical options can be assessed;
  - Contingency responses can be developed; and
  - Durable intelligence information can be assessed before the emergency occurs.

Planning Exercises

The expanding scope and sophistication of emergency operations, along with increased possibilities of acts of terrorism, require agency personnel to quickly act to stabilize and control emergency situations. Proactive emergency planning exercises for these circumstances shall be conducted as follows:

- Documented annual rehearsals and training exercises regarding emergency incidents are essential for all agency personnel to be fully prepared for actual occurrences and special operations;
- Training exercises may involve mock exercises, actual exercises, tabletop exercises, in-service training and/or Troop/Section/Unit training;
- These rehearsals will be used to evaluate the effectiveness, efficiency and applicability of emergency plans in different situations and will include the involvement of those agencies expected to participate in the actual incident;

Planning Exercises, continued

- The Division Commander, designated as lead by the Colonel/Superintendent, will determine the extent, scope, and format for the exercise;
- In the event of an actual implementation of an Emergency Plan due to a natural or man-made disaster incident, the actual implementation of the plan will replace any planned exercise;
- The After Action Incident Report required for all natural or man-made disasters will serve as the critique of the Emergency Plan; and
- A documented analysis and evaluation of any Incident Command System activation incidents, as well as all intra-agency training & rehearsals, will be prepared at least every three years by the Division Commander of Homeland Security and Preparedness or designee.

Annual Training

Troop/Section Commanders shall coordinate annual emergency operations/incident command training exercises. This exercise may be limited to Troop/Section drill, or may include outside agencies such as local police/fire departments, EMS teams, state level response teams, media, non-profit agencies and other entities related to the exercise. When conducted in conjunction with other agencies, the exercise may consist of a tabletop exercise, drill, emergency operations center simulation, or functional exercise involving actual response scenarios.

Troop/Section Commanders shall submit a summary of incident command training exercises conducted to the Emergency Planning Officer no later than October 1st of each year. Upon review by the Division Commander of Homeland Security and Preparedness, the summaries shall be forwarded to the Office of the Superintendent.

The Office of the Division Commander of Homeland Security and Preparedness shall maintain a file of all incident command exercises conducted and may recommend future training or exercises based on prior training or identified need.

Emergency Plan Availability

Any commander may request an existing emergency plan from the Emergency Planning Officer and/or from a Section/Troop headquarters.

Emergency plans containing confidential or sensitive information shall be securely maintained.

Subject:	Number:
Emergency Planning	**SOC-03**

References: ICS Form 205 – Incident Radio Communications Plan;
ICS Form 205A-OS – Communications List;
ICS Form 206 – Medical Plan;
MPAC: 46.1.1, 46.1.2, 46.2.7.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**SOC-03A**

Subject:

Emergency Operations Center (EOC)

Policy

The Department realizes the necessity of an effective response to public safety emergencies as a result of severe weather, terrorist activity, violent protest, natural and/or man-made disasters, through the prudent use of available resources.

Purpose

To provide guidance to personnel regarding the activation and operation of the Department's Emergency Operations Center (EOC).

State Police Emergency Operations Center

The Superintendent/Deputy Superintendent shall activate the EOC when deemed necessary. The EOC shall:

- Coordinate the deployment of Departmental resources in response to an emergency or incident;
- Coordinate the deployment of responding officers to an incident or an incident staging area;
- Direct the security level of response to a potential/actual threat; and
- Operate in conformance with established EOC Guidelines.

State of Emergency

Upon the declaration of a "State of Emergency" by the Governor, the Superintendent/Deputy Superintendent has the authority (within prescribed limits) to commit resources of the Department, or request resources from outside the Department, as deemed necessary, to mitigate the effects of the emergency and to minimize the disruption to public safety.

The Superintendent/Deputy Superintendent shall activate the EOC and shall establish the appropriate security level when necessary.

Upon the declaration of a "State of Emergency" after normal business hours the Watch Center Unit shall immediately notify:

- Superintendent/Deputy Superintendent;
- The EOC on-call personnel;
- Division Commanders; and
- Division of Homeland Security and Preparedness- Emergency Management Unit.

Security Level Guidelines

Upon authorization by the Superintendent/Deputy Superintendent, the EOC shall establish the appropriate security level when necessary. The EOC Director may add, delete, or modify the listed security level procedures in accordance with prevailing circumstances. Security levels and the corresponding response(s) within each level shall be determined by the specific credible information available at that time.

Security Level Procedures

Level	Tasks
I	• ID Check enforced at State Police facilities and identified sites; • Note and report suspicious circumstances, packages and activities; • Ensure building integrity and security; and • Exercise heightened caution when responding to calls for service.
II	*Includes Tasks Assigned At Level I and:* • Implement physical security measures and post security personnel as appropriate; • Identify all vehicles within operational and support areas; • Conduct cursory checks for suspicious items, persons and vehicles as necessary; • Verify and inspect all inbound deliveries and services; • Check delivery and service persons for authenticity with their respective companies; • Exercise extreme caution when responding to suspicious calls for service; • Monitor potential target areas; • All personnel shall wear ID cards in State Police facilities unless in duty uniform; and • Escort all visitors (non-MSP) in State Police facilities.
III	*Includes Tasks Assigned At Levels I , II, and:* • Erect barriers and obstacles (e.g. Jersey Barriers) to control traffic; • Suspend all non-essential contract work or deliveries; • Conduct detailed searches of all operational areas and vehicles; and • Limit or restrict parking around sensitive areas and buildings.

Subject:	Number:
Emergency Operations Center (EOC)	**SOC-03A**

Security Level Procedures, continued

Level	Tasks
IV	*Includes Tasks Assigned At All Levels and:* • Verify the identities of all personnel and need for access; • Deny access to all personnel not associated with local, state or federal agencies; and • Restrict/deny parking in controlled areas.

Responsibilities

Position	Duties
Superintendent/ Deputy Superintendent	Shall: • Review available information provided by the EOC; • Ensure that the Department is operating at the appropriate security level; • Notify the EOC in the event that conditions warrant a change to the existing security level; • Assign the EOC Director; • Authorize the EOC Director to disseminate security level changes throughout the Department; and • Ensure EOC guidelines are developed and kept current.
Emergency Operation Center Director	Shall: • Collect and analyze information regarding Department security levels during personnel redeployment; • Forward recommendations that warrant a change to the Security Level or procedures to the Superintendent/Deputy Superintendent; • Immediately notify the Division Commanders, Commonwealth Fusion Center, Watch Center Unit, and the Emergency Planning Officer of any changes to the security level; • Disseminate security level changes to each Division/Troop/Station/Section/Unit via radio, telephone, internet, fax or any other means as necessary; and • Develop EOC guidelines as directed by the Superintendent/Deputy Superintendent.

Responsibilities continued

Position	Duties
Division Commanders	Shall: • Ensure compliance with the appropriate security level and the established procedures; and • Ensure officers under their command are informed of changes to the security level.
Troop/Station/ Section/ Unit Commanders	Shall: • Notify members who are reporting for duty or members who are re-deployed of the current security level and the established procedure(s) in place.
Sworn/Essential/ Non-essential Personnel	Shall: • Familiarize themselves with the current security level and established procedures.
Commonwealth Fusion Center	Shall: • Provide information to the EOC to assist in situational awareness and development of a common operating picture; • Provide the EOC with a secure, comprehensive mechanism for the timely exchange of information if requested; • Provide the EOC with accurate and timely intelligence products such as bulletins, intelligence and informational briefings, and strategic assessments; • Provide the EOC with direct analytical support for events involving precursor criminal activity; and • Provide the EOC with awareness of priority intelligence requirements and of indicators of threats to the Commonwealth.
Watch Center Unit	Shall: • Provide notification of a State of Emergency as directed by this policy; • Act as the Department's point of contact during a State of Emergency until the EOC is functional; and • Provide assistance to the EOC as directed by the Division Commander of Homeland Security and Preparedness or designee.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**SOC-03B**
Subject:	
Response to Emergency Situations	

Policy

The Department realizes the necessity to effectively respond to public safety emergencies as a result of severe weather, terrorist activity, violent protest, natural and/or manmade disasters, through the prudent use of available resources.

Purpose

To provide guidance for the Department's response efforts to public safety emergencies.

Emergency Operations Center (EOC)

The Superintendent/Deputy Superintendent shall activate the Emergency Operation Center (EOC) when deemed necessary. The EOC shall:

- Coordinate logistics for Troop/Station/Section/Unit personnel redeployment; and
- Operate under established EOC Command Coordination guidelines.

Stages of Personnel Redeployment

The Superintendent/Deputy Superintendent shall authorize the EOC to initiate the following action during the potential threat or occurrence of an emergency/incident.

	If…	Then…
Stage I Redeployment of Personnel	A threat or occurrence of an emergency or incident raises the potential for a shift to be held over or the redeployment of sworn personnel…	• Alert personnel of potential shift hold over and/or prepare for deployment; • Temporarily re-deploy an appropriate number of sworn personnel within the affected Troop(s) and Division; and • Hold over an appropriate number of on-duty sworn personnel.

Stages of Personnel Redeployment, continued

	If…	Then…
Stage II Redeployment of On-Duty Personnel	A threat or occurrence of an emergency or incident creates a situation that is expected to require additional sworn personnel deployment beyond Stage I deployment	• Re-deploy sworn on duty personnel as appropriate from the: o Division of Field Services; o Division of Investigative Services; o Division of Standards and Training; and o Division of Administrative Services.
Stage III Redeployment of All Sworn and Essential Personnel	A threat or occurrence of an emergency or incident requires a full deployment of sworn and essential personnel.	• Deploy all available sworn and essential personnel as necessary; and • The Superintendent/ Colonel may initiate the cancellation of time-off and establish extended work hours as appropriate.

Declaration of State of Emergency

Upon the declaration of a "State of Emergency" by the Governor, sworn and essential civilian personnel (excluding personnel on suspension, injury, or other approved leaves) shall immediately:

- Contact their duty assignment supervisor or other supervising officer within the chain-of-command for specific instructions.

The Superintendent/Colonel may initiate the cancellation of time-off and establish extended work hours as appropriate pursuant to Unit 5A State Police Association of Massachusetts Collective Bargaining Agreement Article 8 § 1D.

Security Level Guidelines

Upon the authorization by the Superintendent/Deputy Superintendent, the EOC may establish a specific security level in conjunction with personnel redeployment or when circumstances dictate. The EOC Director may add, delete or modify security level procedures when necessary. Refer to SOC-03A for security level guidelines.

Responsibilities

Position	Responsibilities
Division Commander	Shall: • Ensure compliance with the appropriate security level procedures; and • Ensure officers under their command are informed of changes to the security level.
Troop/Station/ Section/ Unit Commander	Shall: • Notify members who are reporting for duty or members who are re-deployed of the current security level and the established procedures in place.
Sworn/Essential/ Non-essential Personnel	Shall: • Familiarize themselves with the current Security Level and established procedures.
Incident Management Assistance Team	Shall: • Provide statewide incident management support for all Department emergency operations, on a 24-hour basis; and • Provide Incident Command System (ICS) compliant framework/systems to Incident Commander(s) (IC) when requested.

Emergency Response ICS Framework

The Incident Command System (ICS) provides the basis for response once an incident or event requires more than a single agency response, is multi-jurisdictional, extends into multiple operational periods, or requires the assistance of highly trained and specialized resources to assist in the tactical response and/or management of the incident or preplanned event. Refer to SOC-03D Incident Command System (ICS).

First On Scene

The initial arriving member is critical for assessing the nature and extent of incidents, and for initiating ICS-based response when needed. Upon arrival at the incident, the initial arriving Critical Incident Responder/Supervisor becomes the IC until they are relieved or command is transferred. The initial arriving Critical Incident Responder/Supervisor should ensure that the following critical tasks are initiated:

- Determine nature & scope of incident;
- Establish command & a Command Post (CP). Announce CP location by radio;
- Establish communications with dispatch, Troop Duty Officer and assigned officers;
- Identify and secure the Hot Zone(s). Announce location(s) by radio;
- Establish inner & outer perimeters. Announce locations by radio;

First On Scene, continued

- Request resources as needed. Cancel outstanding request(s) upon arrival of requested resource(s);
- Establish and secure a staging area between the inner & outer perimeters. Announce location by radio;
- Designate a Staging Area Manager. Announce by radio;
- Consider the needs of special populations, including but not limited to:
  - schools,
  - hospitals,
  - nursing homes, and
  - known disabled persons;
- Reassess each step periodically; and
- Designate a Public Information Officer ("PIO") who shall establish and announce by radio the Media Staging Area in consultation with the IC.
  - All media inquiries shall be directed to the PIO ("Speak with one voice").

Incident Commander

Depending on the circumstances, the IC may be a Police, Fire/Rescue, EMS, federal, or other official. Where substantial police and fire/rescue objectives or resources are involved, a Unified Command will often be created, including senior fire and police officials, as well as officials from other public or private sector agencies / organizations with a major stake in the incident.

- NOTE: In the event of a Hazardous Materials incident, a Unified Command must be established. (SARA Act, 1986).

Direction from Incident Commander

All personnel responding to a critical incident, request for assistance, mutual aid request or responding to any critical incident requiring interagency assistance are subject to the direction and control of the IC regardless of the IC's rank, department or agency. This command structure continues for the duration of the event and until the IC is relieved or command is transferred. Supervisors from all departments and agencies are responsible for implementation of this requirement.

Uncontrolled Deployments

Uncontrolled deployments (sometimes referred to as self-deployment or self-dispatching), although initiated with good intentions, can create confusion, cause significant problems at crime and emergency scenes, and can lead to the destruction or inadmissibility of evidence, or injuries to self-dispatching individuals or assigned personnel. These and other forms of unauthorized and/or unreported presence at incidents/events, and unauthorized departures are inconsistent with ICS principals, and may not be eligible for compensation or reimbursement.

Uncontrolled Deployments, continued

The highest-ranking supervisor responding from each agency is responsible for the control and coordination of all personnel from that agency and will coordinate that agency's response with the IC. The responding supervisor is responsible for deploying only the amount of personnel needed and requested by the IC. Department members shall not self-deploy to incidents.

Incident Command Post

The IC shall establish an Incident Command Post ("ICP," can be a building or vehicle) and advise dispatch of that location. Dispatch shall advise all on-scene and responding personnel of that information. The IC shall remain at and operate from the ICP. The IC may move the ICP if its location is threatened by expanding circumstances or hazards. If moved, its new location must be announced immediately to all personnel and to dispatch.

Liaison Officer

The IC shall designate a Liaison Officer, who shall be the point of contact between all Critical Incident Responders and the IC. The Liaison Officer shall meet and brief all responding Agency Representatives at a location to be determined, such as the ICP or the Staging Area.

Staging Area

The IC shall establish a Staging Area between the inner and outer perimeters. It should be large enough to accommodate the required resources and close enough to the incident to make tactical deployments effective and timely. All responding resources shall respond to the Staging Area for check-in unless otherwise directed by the IC. Resources should not respond to the ICP unless directed to do so by the IC or their designee.

Staging Area Manager

The IC shall designate a Staging Area Manager (SAM), who shall have authority for check-in and accountability of Critical Incident Responder arrivals and departures. The SAM will remain in and operate from the Staging Area. All Critical Incident Responders shall report immediately upon arrival to the SAM, and remain in the Staging Area until properly assigned.

Dispatch Notifications

Dispatch shall notify critical incident responder agencies of:

- the location, type and known extent of the emergency;
- the name, rank and agency of the IC;
- the location of and directions to the ICP and the Staging Area;
- the name and agency of the SAM; and
- the name, agency and location of the Operations Section Chief (if a Unified Command is established).

Requesting Assistance

When requesting critical incident assistance, IC, SAMs and dispatchers should scale requests properly.

- Avoid issuing generalized calls for help; and
- Specify by name which agencies are being asked for assistance, how many personnel and any specialized skills needed (e.g.: negotiators, search-and-rescue, entry-team, etc.), along with requested special equipment types.

Reporting to Staging Area

All arriving Critical Incident Responders shall immediately report to the SAM located at the Staging Area for check-in. The SAM shall record the names, rank, agency, specialty, and equipment brought with them on NIMS ICS 211 Check-In-Form or other document.

After arrival and check-in at the Staging Area, one supervisor from each responding agency should report to the ICP or other location designated by the IC or Liaison Officer. That individual will serve as the responding agency's representative. That person should have authority delegated from their agency to make decisions on the deployment of their agency resources.

The SAM must carefully consider where arriving personnel are to park their vehicles. Blocking of streets, bridges, underpasses, etc., may hinder rapid arrival of essential emergency vehicles. Arriving personnel shall park where designated by the SAM.

Arriving personnel shall remain at the Staging Area until assigned by the IC or relieved.

Demobilization

Personnel located at the Staging Area who intend to demobilize from the incident shall contact the SAM and await SAM authorization before departing.

Demobilization, continued

Agency Representatives wishing to demobilize their resources from the incident shall contact the Liaison Officer and await Liaison Officer authorization before departing; demobilization must be accomplished through and according to the direction of the SAM.

A proper demobilization plan shall be completed to accurately record departing personnel and resource check-out time, notation of any apparent physical injuries or critical incident stress-related concerns, and include notations of any damaged or lost equipment. NIMS ICS 221 Demobilization Check-Out Form or other suitable document should be utilized.

Unified Command

A determination must be made promptly whether to continue under an IC, or via establishment of a Unified Command. If a Unified Command is established, a single, coordinated Incident Action Plan (IAP) must be agreed upon, and an Operations Section Chief designated by agreement to implement it. The IC remains in command until relieved by the Unified Command.

The IC or Unified Command must delegate the Planning Section Chief (PSC) to begin or expand the planning process by developing a single consolidated Incident Action Plan with appropriate NIMS ICS 204 Assignment forms for each responding resource that will be assigned to a Division or Group Supervisor, or Strike Team or Task Force Leader.

ICS Support

All supervisors from Critical Incident Responder agencies have a continuing duty to support ICS-based operations, particularly with regard to unity of command, for the duration of the incident or event.

References:

SOC-03A – Emergency Operation Center (EOC);
The National Incident Management System (NIMS);
Commonwealth of Massachusetts "Recommended Protocol For Managing Initial Response To Critical Incidents, April 2014";
MPAC: 81.2.5.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**SOC-03C**
Subject	
Response to Civil Disturbances	

Policy

The Department realizes the necessity of an effective response to any civil disturbance through the prudent deployment of available Departmental resources.

Department members assigned to a civil disturbance or planned mass demonstration duty shall ensure all issued riot gear is accessible and operational, including a riot helmet with the member's identification number clearly displayed. Any deficiencies noted upon assignment arrival shall be immediately reported to the on-scene supervisor.

Department members shall receive initial training, and annual training thereafter, related to Department response to civil disturbances.

According to Massachusetts General Laws c.269 §1:

- An unlawful assembly exists when five or more persons, being armed with clubs or other dangerous weapons, or ten or more persons, whether armed or not, are unlawfully, riotously, or tumultuously assembled; and
- An "Order to Disperse" shall be given to persons unlawfully assembled before any action can be taken against them.

Definitions

Commission: The Massachusetts Peace Officer Standards and Training (POST) Commission as established in M.G.L. c.6E § 2.

De-escalation Tactics: Proactive approaches to stabilize a law enforcement situation so that more time, options, and resources are available to gain voluntary compliance and reduce or eliminate the need for force. These approaches may include, but not be limited to:

- Verbal persuasion;
- Warnings;
- Slowing down the pace of an incident;
- Waiting out an individual;
- Creating distance between the member and a threat;
- Requesting additional resources, including, but not limited to licensed medical or mental health professionals, as defined in M.G.L. c. 111 § 51 ½ (a), when appropriate, to address a potential medical or mental health crisis; and
- Issuing a summons as an alternative to arrest where feasible.

Kettling: Confinement or corralling by law enforcement of a group of demonstrators or protestors in a small area without any means of egress as a method of crowd control, management or restraint.

Tear Gas or Other Chemical Weapons (CW): Any weapon that contains chemical compounds that temporarily make people unable to function by causing irritation to the eyes, mouth, throat, lungs, and skin, or that otherwise restrain a person by causing pain. This shall not include oleoresin capsicum (OC) spray.

Civil Disturbances Initial Inquiries

Whenever any law enforcement agency requests the assistance of the Massachusetts State Police for mass demonstrations, civil disorders, riots, etc., a request to such effect shall be made through channels to the Office of the Superintendent/Deputy Superintendent. The following minimum information is required:

- Requesting department, rank and name of the caller;
- Name of authorizing official and a call-back number;
- Specific facts surrounding the incident:
  - Location;
  - Number of officers on-scene/enroute;
  - The reason or purpose for the disturbance; and
  - Number of people causing the disturbance and whether armed, violent, or hostile.

Planned Mass Demonstration

When the Department obtains advance knowledge of a planned mass demonstration, the Operations Officer in the Troop of Jurisdiction shall:

- Diligently attempt in good faith to communicate with organizers of the event before the event occurs in an effort to establish reliable channels of communication between Department members and event participants;
- Discuss and establish logistical plans to avoid or, if necessary, to de-escalate potential or actual conflict between law enforcement officers and mass demonstration participants; and
- Be designated as the Department officer-in-charge of de-escalation planning and communication to carry out the above plans for the planned mass demonstration.

Civil Disturbances Response

The "Order to Disperse" shall be given by the Incident Commander (IC) at the scene. The restoration of public peace should be accomplished first through persuasion. If necessary, force may be employed.

The use of Kettling as a means of crowd control, crowd management, or crowd restraint is prohibited.

Crowd control objectives:

- Protect life and property;
- Contain and isolate the disturbance;
- Disperse as expeditiously as possible;
- Prevent re-grouping or re-entry; and
- Identify and take action against law violators.

Officers shall keep in mind the limitations imposed upon the Department in private business sector strikes in accordance with ADM-04 State Police Authority.

Responsibilities

Position	Duties
Responding Officer	Shall: • Report with the current duty uniform and riot gear; • Report to the IC on-scene for instructions when responding in plainclothes; • Be issued additional restraining devices, as necessary, by the Supply Section; • Field search detainees prior to entering an established Field Processing Area; and • Submit all appropriate reports using the incident case number as issued by the IC.
On-scene Department Incident Commander	Shall: • Order or verify that an "Order to Disperse" (PowerDMS- Bulletins-Dispersal Order) was issued to all persons to immediately and peaceably disperse; • Take necessary action if the crowd fails to disperse after being ordered to do so; • Request additional personnel and support through the Division Commander of Field Services; • At no time attempt to accomplish a police objective, unless sufficient forces are present to support such objective; • Establish a Field Processing Area when necessary; • Assign officers (e.g., security, intake, booking, evidence control, photo/ fingerprint, court officer, clean-up, etc.) as needed, to maintain a Field Processing Area; and • Prepare and submit an "After Action Report" within 24 hours after termination of all Departmental activities.

Responsibilities, continued

Position	Duties
Division Commander of Field Services	Shall: • Ensure adequate uniformed personnel and tactical support remain in the affected area during and after order is restored for such period of time as deemed necessary by the Colonel/Superintendent; and • Ensure any further disruptions are addressed as expeditiously as possible.

Use of Chemical Munitions During Civil Disturbances

Use of chemical munitions is governed by STOP Team SOP's in accordance with 550 CMR 6.08 (3-4), specifically:

- A member shall not discharge or order the discharge of tear gas or any other chemical weapon, discharge or order the discharge of a kinetic impact device or rubber pellets from a propulsion device to control or influence a person's behavior unless:
    - De-escalation tactics have been attempted and failed or are not feasible based on the totality of the circumstances; and
    - The measures used are necessary to prevent imminent harm and the foreseeable harm inflicted by the tear gas or chemical weapon, kinetic impact device, rubber pellets is proportionate to the harm.
- If a law enforcement officer utilizes or orders the use of kinetic impact devices, rubber bullets, Conducted Energy Devices (e.g. Taser) , Chemical Weapons(CW), or Electronic Control Weapons (e.g. Taser) against a crowd, the law enforcement officer's appointing agency shall file a report with the Commission detailing all of the measures that were taken in advance of the event to reduce the probability of disorder and all de-escalation tactics and other measures that were taken at the time of the event to de-escalate tensions and avoid the necessity of using said weapon(s), including a detailed justification of why use of said weapon(s) was objectively reasonable.

Use of Canines During Civil Disturbances

Use of Canines is governed by the Canine Unit SOP's in accordance with 550 CMR 6.08 (4-5), specifically:

- A member may not order the release of a dog to control or influence a person's behavior unless:
    - De-escalation tactics have been attempted and failed or are not feasible based on the totality of the circumstances; and
    - The measures used are necessary to prevent imminent harm and the foreseeable harm inflicted by the release of the canine is proportionate to the harm.
- If a law enforcement officer utilizes or orders the release of a dog against a crowd, the law enforcement officer's appointing agency shall file a report with the POST Commission detailing all of the measures that were taken in advance of the event to reduce the probability of disorder and all de-escalation tactics and other measures that were taken at the time of the event to de-escalate tensions and avoid the necessity of using said weapons, including a

Use of Canines During Civil Disturbances, continued

detailed justification of why use of said weapons was objectively reasonable.

- Canines should not be utilized for crowd control, restraint, or management of peaceful demonstrations, but may be deployed for crowd control, restraint, or management of peaceful demonstrations in isolated circumstances related to bomb detection, pursuit of suspects in buildings, and related situations. Utilization does not include circumstances in which the canine remains on a short lead in close proximity to the handler and is well behind the line of contact between law enforcement and civilian personnel.

Mass Arrests Logistics

The following procedures, and requirements of DET-06 Detainee Monitoring, shall be used when a situation requires multiple arrests:

- Normal arrest procedures shall be used for all arrested individuals;
- All arrested individuals shall be subject to the appropriate bail procedures;
- Arrested individuals shall be expeditiously taken to a Field Processing Area;
- For record keeping purposes and whenever feasible, the arresting officer’s name shall be written on the photograph of each individual they have arrested;
- As soon as possible, transport arrested individuals to an appropriate place of temporary confinement or released after booking as directed by judicial authorities;
- Food, water, medical and sanitation needs shall be tended to as soon as reasonably possible;
- The face sheet/arrest report and Detainee Property Inventory Form shall be sent with the transporting officer to the place of confinement or release;
- The court of jurisdiction and the appropriate District Attorney's office shall be apprised of the situation; and
- Contraband or evidence shall remain with an assigned Evidence Control Officer.

Subject:	Number:
Response to Civil Disturbances	**SOC-03C**

After Action Report

An After Action Report shall be prepared by the IC assigned to the scene. It shall begin with a numerical, chronological listing of all arrested individuals and shall contain, at a minimum:

- Number and source of complaints;
- Verbatim instructions given to the crowd and the name of the officer giving them;
- Department personnel on scene and their respective duties;
- Names of arresting officers and individuals arrested;
- Contraband and evidence seized;
- Damage to private/public property;
- Injuries to police/public; and
- Private/public agencies/personnel involved.

References: ADM-04 State Police Authority;
DET-06 Detainee Monitoring;
MGL c.269 §1;
550 CMR 6.08 *et seq.*;
MPAC: 46.1.2, 46.1.11, 46.1.12.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**SOC-03D**

Subject:

All Hazards Incident Command Framework

Policy

Members shall use the incident management strategies outlined in this policy for all multi-agency and multi-jurisdictional responses. In addition, and when applicable, members are encouraged to use these strategies for responses to incidents involving only the Department.

Purpose

To provide guidance for the Department's response efforts to emergencies and incidents.

Incident Command System Defined

Incident Command System (ICS) is an "all risk" emergency incident management system used for managing a wide variety of emergencies.

The Federal Emergency Management Agency (FEMA) defines ICS as: "An incident management system consisting of procedures for organizing personnel, facilities, equipment, and communications at the scene of an emergency."

ICS provides a common organizational structure, or framework, within which participating agencies can work toward accomplishing common goals and objectives. While the system works well in all types of emergency incidents, its primary benefit is found in managing incidents of a multiagency or multi-jurisdictional nature.

The federal government requires an ICS to be used at the scenes of hazmat incidents. This regulation has been promulgated by the Occupational Safety and Health Administration (OSHA) at 29 CFR 1910.120.

Major Components of the Incident Command System

- Common Terminology: Responding agencies can communicate at the scene of an emergency only if they have a common understanding of the terminology used by the various emergency responders. Common names are established and used for personnel, equipment, and facilities operating in and around the incident area.

- Modular Organization: An incident management system is valuable only if it can adapt to changing conditions at the scene of an incident. A common characteristic of emergency situations is that they seldom remain constant; the incident often will expand or contract. A modular organizational structure will allow the incident response to grow in direct proportion to the complexity of the incident. Conversely, the structure of the response can be scaled back as conditions improve and resources are no longer needed.

- Integrated Communications: Effective communications at the scene of an incident are essential for proper incident management. Whenever possible, responding agencies should be able to talk directly to each other through common radio channels. Furthermore, command personnel must be able to personally interact to formulate effective response strategies.

- Command Structure: ICS recognizes the key ingredient to any emergency response is to have an effective command structure to manage personnel and other resources. The command function may be organized in one of two ways:

    - A *single command* involving one person may be used when there is no overlap of jurisdictional boundaries or when a single commander is designated by the agency with overall management responsibility for the incident. This person is normally referred to as the Incident Commander (IC).
    - Under a *unified command* structure, all involved agencies contribute to the command process by sharing management responsibility. A unified command structure is the preferred method when responding to emergencies of a multiagency or multi-jurisdictional nature. Even with a unified command structure, however, one person will still be in overall charge of the event.
- Span of Control: Span of control is defined as the number of subordinates one supervisor can manage effectively. ICS recommends that one person can properly supervise no more than three to seven subordinates, with the optimum number being five. Command officers must anticipate span of control problems and prepare for them as the modular organizational structure of the incident response expands.

- Consolidated Action Plan: ICS requires every emergency response to have a consolidated action plan.
    - For small incidents, this may be something as simple as the IC having a cognitive plan. For large scale events, the incident response may require a written plan, even as the event is unfolding.

Major Components of the Incident Command System, continued

- ICS requires all plans to address strategic goals and tactical objectives.
  - Strategic goals are broad in nature.
  - Tactical objectives are the tasks that must be accomplished to achieve strategic goals. Objectives are specific and measurable.

- Designated Incident Facilities: ICS recognizes that designated incident facilities can greatly assist the IC in managing the incident. For instance, a Command Post is designated to serve as the on-scene location from which all incident operations are directed. Similarly, staging areas are established to designate where available resources should report for assignment. Other facilities are established as the need arises.

- Comprehensive Resource Management: The IC is responsible to ensure all resources currently available are used effectively and efficiently. Resource management requires that the safety of personnel is given the highest priority. The IC must continually evaluate and adjust the deployment of resources at all incidents. If additional resources are needed to manage the incident, the IC must ensure they are obtained in a timely manner.

Incident Command System Functional Areas

The organizational structure of ICS requires the establishment of five key functional areas. In a small, single command structure, the IC will be able to perform all five functions. In a large scale event, however, the IC will designate section chiefs to manage the responsibilities of the various areas.

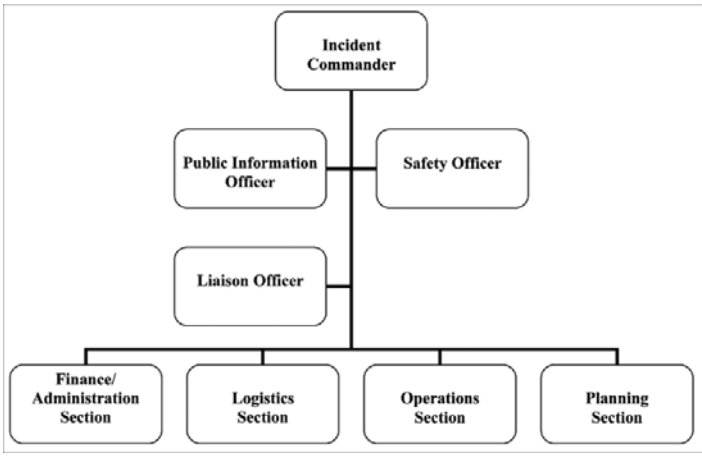
Command

Incidents are commanded by an IC, normally from the agency having primary jurisdiction, who is responsible for the management of all incident operations. As previously discussed, command may be established either through a single or unified command structure. The IC is responsible for the following activities:

- Assessing incident priorities;
- Determining strategic goals and tactical objectives;
- Developing and implementing the incident action plan;
- Developing an appropriate organizational structure;
- Managing resources;
- Coordinating overall emergency activities;
- Ensuring scene safety, proper liaison with other agencies; and disseminating information to the news media.

Incident Command System Functional Areas, continued

NOTE: In some large scale events, the IC must delegate authority to ensure the above responsibilities are properly addressed. Any functions not specifically delegated by the IC remain the responsibility of the IC. Any one or all of the functional areas depicted in the following diagram may be established as the need arises.



Operations Section

The Operations Section is responsible for the management of all tactical operations at an incident. The most common reason for staffing operations is to relieve span-of-control concerns for the IC. Some incidents may become so complex that the IC may no longer be able to solely supervise all operational aspects of an incident. An Operations Section Chief will be able to assist the IC by:

- Assisting in development strategic goals and tactical objectives for the incident;
- Developing operational plans;
- Requesting or releasing resources through the IC;
- Consulting with the IC about the overall incident action plan;
- Keeping the IC informed of the progress of the incident and the status of resources; and
- Supervising the Staging Area Manager.

Incident Command System Functional Areas, continued

Planning Section

The Planning Section is responsible for the collection, evaluation, dissemination, and use of information about the development of the incident and the status of resources. Planning includes an assessment of the current situation and a projection of future conditions. Members in the Planning Section maintain information about resources committed to the incident and projected resource requirements. The modular nature of ICS also allows the planning function to be expanded in scope to include the following Subdivisions or Units:

- Resource Unit: The Resource Unit provides answers to the following questions which are important to the IC: What resources (personnel and equipment) are currently committed to the incident? Where are these resources assigned? Are all personnel accounted for at shift changes? Are additional resources necessary? Where can they be obtained?

- Situation Analysis Unit: Members in the Situation Analysis Unit analyze the incident as it progresses. They help the Planning Section Chief and the IC develop a consolidated action plan and determine if the plan is being followed and whether the plan of action is having the desired effect. Members of this Unit will also offer alternatives to the IC in those situations where the original plan must be modified.

- Documentation Unit: The Documentation Unit is responsible for recording the incident and protecting all documents relevant to the incident. Examples include Incident Reports, Communication Logs, CLEAN Messages, Injured Employee Statements, correspondence, and directives from various sources. In all incidents, thorough documentation is essential to permit proper after-action analysis. In major emergency incidents, a member should be assigned to collect information for the After-Action Report while the incident is still ongoing. This will ensure the availability of appropriate documentation for reporting purposes and will also ensure a timely completion of the After-Action Report.

- Demobilization Unit: The Demobilization Unit should begin preparing for the orderly and controlled withdrawal of resources from the scene of the emergency while the incident is still unfolding. This will ensure that resources are properly managed and that the scene is returned to a state of normalcy as soon as possible after the incident has terminated.

Incident Command System Functional Areas, continued

- Technical Specialists: Technical specialists should be included in the planning function whenever expertise is needed beyond the levels maintained by the IC and their immediate subordinates. Examples include hazmat personnel, engineers, industry representatives, explosives technicians, and radiation experts.

- CISM: Crisis Incident Stress Management Team personnel should also be included in the planning function.

Logistics Section

The Logistics Section is responsible for providing facilities, services, and materials to sustain the incident response. The logistical needs of the members assigned to an incident will grow in direct proportion to the size, duration, and complexity of the incident. The Logistics Section Chief may elect to establish functional Units to perform the following roles:

- Communications Unit: The Communications Unit will perform a vital role by developing and overseeing the operation of the communications infrastructure. Members of this Unit will ensure that proper equipment is available and that it is performing to acceptable standards. They will maintain the operational readiness of all radio, telephone, and CLEAN System communications at the Command Post and other incident facilities.

- Facilities Unit: The Facilities Unit will ensure the availability of adequate buildings and shelter for incident operations. Included in this category are such matters as Command Post location and operation, feeding and housing areas, sanitary facilities for field operations, and other fixed facilities necessary for the successful management of the incident.

- Procurement and Supply Unit: This Unit orders the equipment and supplies required for incident operations and maintains ongoing inventory and control of these resources. Examples in this category include clerical supplies such as paper and pens, as well as tactical supplies such as ammunition and tear gas.

- Food Unit: Incidents that operate for an extended period of time will require the procurement of food for participating personnel. In smaller incidents, this role may be handled within the Procurement and Supply Unit, e.g., when sandwiches are obtained for a 12-hour operation. However, for incidents that may extend for days, the IC and Logistics Section Chief may elect to contract food services from a local vendor. A Food Unit within the Logistics Section would be responsible for making the necessary arrangements.

Incident Command System Functional Areas, continued

- Other Service and Support Units: Other service and support Units can be added to the Logistics Section as the need arises.

Finance/Administrative Section

The Finance/Administrative Section is responsible for tracking all incident costs and evaluating the financial considerations of the incident. Financial considerations for a major Department mobilization can be extensive, especially when the Department tries to seek reimbursement for the operation or when detailed records must be prepared for budgetary or planning purposes. The Section Chief has the responsibility to document all incident costs and to provide guidance to the IC on financial issues that impact incident operations. As with other functional areas, the Finance/Administrative Section can be subdivided into Units to manage matters such as timekeeping, billing, and cost accounting.

Expansion: Not all of the above functional areas may be needed during an incident response. However, IC(s) must be prepared to expand their organizational structure if the need arises.

Incident Priorities

A member serving in the capacity of the IC has numerous duties and responsibilities to perform. These responsibilities will vary depending upon the nature of the incident and the number of available resources. One aspect of the emergency response that will not vary, however, is the recognition of three incident priorities. *Regardless of the nature of the incident, the following priorities WILL ALWAYS be addressed in an emergency incident response:*

- Life Safety: Life safety is the first priority for any emergency incident. This includes not only the safety of any victims involved in the incident, but also the safety of response personnel and populations surrounding the incident scene. IC(s) must place life safety above all other considerations of emergency incident management.

- Incident Stabilization: The IC's second priority is to formulate a strategy to stabilize the incident. Incident stabilization involves the development of a plan to minimize the effect the incident may have on the surrounding area and populations (e.g., with incidents of civil disorder, this priority will involve isolation of the perpetrators and containment of the disorder to prevent it from spreading; a hazmat response team might stabilize an incident by containing the spill at the scene of a crash and preventing runoff into nearby waterways).

Incident Priorities, continued

- Property Conservation: Property conservation involves achieving strategic goals and meeting tactical objectives at an incident while minimizing property damage and inconvenience to uninvolved citizens. While this priority is clearly important, it should not weigh as heavily with the IC as the previous priorities of life safety and incident stabilization. Nevertheless, an emergency incident cannot be considered successfully managed if the IC does not give this priority proper consideration.

NOTE: In addition to the above priorities, restoration of traffic flow for incidents occurring on or around highways must be considered when normal traffic patterns are disrupted. Major highway incidents often create substantial disruptions to traffic, and it is the responsibility of the IC to restore normal or limited traffic flow around the scene as soon as possible. Refer to TRF-05 Traffic Incident Management for additional guidance.

Incident Command Summary

When using the ICS, members must be cognizant that the system is a management tool. ICS does not replace sound command decision making at the scene of an incident; it does not avoid the need for proper training and education; and it does not eliminate the need for establishing positive interagency relationships. The system does provide a broad management framework under which one agency or many agencies can operate at the scene of an emergency.

ICS makes the best use of available resources. Resources are essential to the management of any emergency incident. Some incidents, such as a minor non-reportable motor vehicle crash, can be managed with no resources other than the member assigned to make a record of the crash. Other incidents, such as a major civil disturbance, may require hundreds of personnel resources and dozens of pieces of equipment to successfully resolve the incident. ICS helps the on-scene commanders manage the resources at their disposal.

ICS does not, in any way, cause an agency to relinquish authority at the scene of an incident. On the contrary, this system recognizes the valid role that all emergency response agencies play at the scene of an incident. ICS further establishes a system in which the various responders can perform their individual roles in a unified manner with the other agencies represented at the scene.

Incident Command Summary, continued

ICS can be effective only when all members of an organization practice ICS principles in their day-to-day responses to emergency situations. ICS works best when members apply the principles taught in training to small, frequently occurring events, such as traffic collisions and minor crime scenes. As a result of this constant repetition and familiarity, members are then better able to manage the large-scale events such as civil disturbances and motor vehicle crashes involving multiple fatalities. ICS operating principles become so well established that they soon become an integral part of all incident management.

ICS Support

All supervisors from Critical Incident Responder agencies have a continuing duty to support ICS-based operations, particularly with regard to unity of command, for the duration of the incident or event.

For incidents falling within the primary jurisdiction of the Department, the highest ranking Department member at the scene shall assume the role of IC. However, to ensure command continuity, the temporary involvement of a higher-ranking member at the scene will not automatically require that member to assume the role of IC. If, in the opinion of the higher ranking member, the situation dictates that he/she remain at the scene, then the higher ranking member shall assume the role of IC.

Supervisors shall monitor the status of all incidents and ensure that an appropriate management strategy is employed.

ICS Training

The Commandant of the State Police Academy shall ensure Basic Incident Command System training is made part of the Recruit Training Curriculum.

References: TRF-05 Traffic Incident Management;
29 CFR 1910.120;
The National Incident Management System (NIMS);
MPAC: 46.1.2, 46.1.3, 46.1.4, 46.1.5, 46.1.6, 46.1.7.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**SOC-03E**

Subject:

Emergency and Continuity Plan Requirements

Policy

In accordance with SOC-03 Emergency Planning, and SOC-03D All Hazards ICS Framework, the Department shall maintain written plans for responding to critical incidents including, but not limited to, natural and man-made disasters, pandemics, civil disturbances, mass arrests, bomb threats, hostage/barricaded person situations, acts of terrorism, and other unusual incidents. These plans will follow standard Incident Command System (ICS) protocols and National Incident Management System (NIMS) which include functional provisions for: Command, Operations, Planning, Logistics and Finance/Administration.

Sworn members shall receive annual training on the All-Hazards Plan of the Department.

Purpose

To provide specific guidance for the Department's plans for emergencies and continuity of operations.

Emergency Planning Manual Content

The Emergency Planning Manual is a collection of all of the Department's major emergency plans. The Emergency Planning Manual shall include:

- All current Emergency Operating Plans (EOPs);
- Incident Action Plans (IAPs);
- Operational guidelines;
- On-site operational instructions; and
- Personnel, equipment, and resource inventories.

Emergency Operation Plan Content

The EOPs should contain general objectives reflecting the overall strategy for responding to and managing critical incidents. These plans define the scope of preparedness and incident management activities required of the Department and are flexible enough for use in all emergencies. These plans include resource inventories and other necessary information, including but not limited to:

- Personnel and skills;
- Department property, buildings, and vehicles;
- Supplies (food, fuel, clothing);
- Arrest/confinement procedures;

Emergency Operation Plan Content, continued

- Topographical maps;
- Support equipment;
- Incident Command Posts;
- Field Command Posts;
- Communications;
- Miscellaneous Equipment (generators, boats, etc.); and
- Forms including After-Action reporting, ICS Forms 205, ICS 205A-OS, ICS 206, and Identified Staging Areas.

ICS Command Structure Integration

EOPs shall integrate the ICS Command Structure pursuant to established Department SOC policies and NIMS framework recognizing that all functions without an appointed Section Chief are the responsibility of the Incident Commander.

The following functions are part of the ICS system and the roles/responsibilities of each when activated include, but are not limited to the following:

Command Function

- Activating the incident command system;
- Establishing a command post;
- Initiating the notification and mobilization of additional agency personnel;
- Obtaining support from other agencies;
- Establishing a staging area, if necessary;
- Providing public information and maintaining media relations;
- Maintaining the safety of all affected personnel; and
- Ensuring a documented after action report is prepared.

Operations Function

- Establishing perimeters;
- Conducting evacuations;
- Maintaining command post and scene security;
- Providing for detainee transportation, processing, and confinement;
- Directing and controlling traffic; and
- Conducting post-incident investigation.

Planning Function

- Preparing a documented incident action plan including, when applicable, what will trigger implementation of the plan;
- Gathering and disseminating information and intelligence; and
- Planning post-incident demobilization.

ICS Command Structure Integration, continued

Logistics Function

- Communications;
- Transportation;
- Medical support to include support for emergency response personnel;
- Supplies; and
- Specialized team and equipment needs.

Finance/Administration Function

- Recording personnel time;
- Procuring additional resources;
- Recording expenses; and
- Documenting injuries and liability issues.

Continuity of Operations Plans

To ensure the Department is prepared to provide required services, even if affected by significant emergency, Stations/Sections/Units shall follow a Continuity of Operations Plan (COOP) to ensure the continued performance of essential functions during a wide range of potential emergencies.

In the event of an incident requiring relocation of services, the Station/Section/Unit Commander shall notify their Division Commander who shall communicate the incident and needs to the Colonel/Superintendent. This notification shall include details on the incident, affected services, operational impacts, operational requirements, personnel requirements and other information required to provide the resources necessary to continue the operations of the affected Station/Section/Unit.

The Division Commander shall, at the direction of the Colonel/Superintendent, coordinate with the Division of Administrative Services who will coordinate and approve requests for recovery planning resources that fall outside the scope of an individual Station/Section/Unit to ensure the relocation is safe, effective and the interruption to normal operations is minimal. The security and protection of evidence storage areas and data infrastructure shall be prioritized.

Recovery Planning

Station/Sections/Units should coordinate with the Division of Administrative Services the pre-positioning of minimum essential equipment at an alternate identified facility when advance warning of an emergency is received.

Personnel Issues: Commanders should plan to provide critical information to both essential and non-essential staff to inform employees on how to prepare themselves and their families prior to an emergency.

Evidence/Contraband/Property (ECP): Commanders should plan for the security and integrity of all ECP and take steps to mitigate the impact to ECP operations.

Recovery Planning, continued

Vital Records and Communications

Commanders shall provide for the protection and availability of electronic and hardcopy (as applicable) of documents, references, records, information systems, and databases.

Safekeeping of systems and data is critical to alternate operations, so Commanders should:

- Identify vital records, systems, and data (hard copy and electronic) critical to performing functions including:
  - Emergency operating records – plans and directives, orders of succession, delegations of authority, staffing assignments; and
  - Legal and financial records – personnel records, Social Security records, payroll records, retirement records, insurance records, contract records;
- Plan for protection, duplication, and movement of records;
- Ensure accuracy and currency of records, update as necessary;
- Ensure procedures for documenting operations when COOP is activated;

Communication systems are critically important, and are often severely impacted in times of disaster. Commanders should plan for the loss of one or more routine communications system and have an alternate or workaround identified. Commanders should also be aware that in time of disaster cellular communications systems are often the first system to fail.

Reconstitution and Termination

The Colonel/Superintendent, or designee, shall communicate to affected personnel the termination of alternate operations and returning to a non-emergency status at the primary facility at the conclusion of the incident. This communication should inform all personnel that the emergency no longer exists and provide instructions for resumption of normal operations.

Guidance and Assistance

Additional guidance documents to help prepare Emergency Operation and Continuity of Operation plans are available through the EPO.

Responsibilities

Position	Duties
Colonel/ Superintendent	Shall: • Ensure a designee reviews and approves Department-wide Emergency and COOP plans as maintained by the EPO.
Division Commanders	Shall: • Ensure the Division's planning personnel annually review and update Division Emergency and COOP plans; • Review and forward revisions of Division Emergency and COOP plans to the EPO; and • Review quarterly status reports of the Division's emergency equipment inventory.
Troop/Section/ Unit Commanders	Shall: • Conduct a quarterly inspection (January/April/July/October), for operational readiness of equipment designated for use in support of their EOP/COOP plans as specified by the EPO, and document all inspections in the records management system(s) as required by the EPO; and • Notify their respective Division Commander of any deficient inspection results.
Emergency Planning Officer (EPO)	Shall: • In accordance with SOC-03, maintain copies of all Emergency plans and also maintain copies of relevant COOP plans; • Provide updated Emergency and COOP planning initiatives to Division planning personnel as available; • Annually request Divisions review and update as necessary existing Emergency and COOP plans. • Revise Department COOP priorities to coincide with Division updates; • In concert with the Division of Administrative Services, ensure a master database of the emergency equipment necessary to carry out the Department's Emergency and COOP plans is maintained and updated quarterly. This shall include a detailed inventory, location and status of said equipment; • Annually issue a list of equipment deemed necessary to maintain the Department's continuity abilities and response to emergencies, and ensure quarterly inspections are carried out on the equipment by the appropriate Station/Section/Unit Commanders; and • Notify the Division Commander of Administrative Services of any emergency equipment deficiencies.

Subject:	Number:
Emergency and Continuity Plan Requirements	**SOC-03E**

References The National Incident Management System (NIMS);
MPAC: 46.1.2, 46.1.3, 46.1.4, 46.1.5, 46.1.6, 46.1.7, 46.1.8, 46.1.13.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

2071

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**SOC-04**
Subject:	
Lost/Missing Person Searches	

Policy

Every incident involving a lost and/or missing person shall be treated as a potential emergency event that may require a rapid and coordinated response of specialized personnel and equipment.

Members should understand that every lost and/or missing person incident has the potential of being or becoming a criminal investigation; members shall treat the scene of each incident as a potential crime scene.

If the missing person is identified as a child of age seventeen (17) or younger and there is evidence of abduction, notify the AMBER Alert Activator and follow procedures in accordance with SOC-04A AMBER Alert Activations.

Public notifications/messaging for missing persons not fitting Amber Alert criteria shall be coordinated through channels to Media Relations.

Stage One Response Protocol

Upon receiving a report of a lost/missing person and/or receiving a request for Department assistance in locating a lost/missing person, the Desk Officer shall immediately gather as much information as possible, including, but not limited to:

- Reporting person's information;
- Name, age, and address of the missing person;
- Description of appearance/clothing;
- Activity at time of disappearance;
- Place Last Seen (PLS);
- Physical or general health condition;
- Any mental or cognitive deficiencies (e.g., Alzheimer disease, dementia, or autism);
- Does the missing person have an electronic tracking transmitter;
- Involvement of any weapon;
- Requesting agency point of contact including their call back telephone number; and
- Action(s) taken so far.

Stage One Response Protocol, continued

Position	Duties
Desk Officer	• Dispatch the appropriate patrols; • Notify the Troop Duty Officer of all requests; • Broadcast all pertinent information over the radio; and • Make appropriate Daily Administrative Journal (DAJ)/ACISS entries.
Troop Duty Officer	• Dispatch a supervisor to the scene; • Dispatch K-9 to the scene; • Advise the Air Wing of the situation and ascertain availability if services are required; • Dispatch an available SERT member working in the Troop to the scene; • If the missing person is equipped with an electronic tracking transmitter, dispatch Department members equipped with electronic tracking receivers; • Dispatch other resources as needed; • Ensure that a SP 622 Lost/Missing Person Questionnaire is completed by on-scene personnel; • Conduct an assessment of the "search urgency" by reviewing the current information. The following conditions may indicate a high search urgency: o Child under twelve (12) years of age; o Adult over seventy (70) years of age; o Mentally challenged individuals; o Physical conditions or health issues; o Extreme or deteriorating weather conditions; o Time of day; o Forecast weather conditions; o Persons determined to be at risk to themselves; and o Other pertinent factors; • Make appropriate DAJ/ACISS entries; and • Notify the Troop Commander

Stage Two Response Protocol

A Stage Two Response Protocol is based upon the need for a more comprehensive response as determined by:

- The requesting agency;
- The responding members; or
- Based upon a search urgency analysis.

The Troop Duty Officer shall request, through the GHQ Communications Section, that the Special Operations Commander or designee be contacted for a Stage Two Response. The Special Operations Commander or their designee must approve the request prior to any Stage Two Response activation orders.

When authorized, the Special Operations Commander or designee shall activate additional resources as needed (e.g., SERT, IMAT, Air Wing, K-9, Mounted, etc.).

Outside agencies (e.g., Environmental Police, Department of Conservation and Recreation, etc.) may be authorized by the Troop Duty Officer after consultation with the Special Operations Commander or designee.

Other resources (e.g., Civilian Search and Rescue Teams, Volunteers, etc.) shall only be authorized by the Special Operations Commander or designee.

Follow-up Investigation

The on-scene Supervisor or a Department member acting as the primary investigator will ensure there is follow-up contact with the reporting party or source of information. Follow up searches may be warranted for evidence or other circumstances dictated by the incident.

The State Police Detective Unit (SPDU) of jurisdiction will be notified in the following instances:

- The missing person is not located after an extended period of time;
  - The extended time period is situationally dependent upon circumstances directly related to the specific incident.
- The person is missing under suspicious circumstances;
- There is evidence of a potential crime;
- The missing person was located and has sustained serious bodily injury that has or may result in death; and
- Other reason(s) as determined by the on scene Supervisor.

The missing person should be entered into CJIS and NCIC by the primary investigating agency. Once located, the missing person should be removed from those databases by the primary investigating agency.

Subject:	Number:
Lost/Missing Person Searches	**SOC-04**

Reference SOC-04A Amber Alert Activations;
TOP-01 Special Operations Command and Control;
SP 622 Lost/Missing Person Questionnaire;
MPAC: 41.2.5.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

2075

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**SOC-04A**
Subject:	
AMBER Alert Activation	

Policy

The Department is the sole entity within the Commonwealth permitted to initiate an America's Missing Broadcast Emergency Response (AMBER) Alert for cases of child abduction where the child's life is in imminent danger of serious bodily harm, injury, or death and specific criteria supporting the AMBER Alert activation has been met.

MSP Operations at GHQ, 508-820-2121, is the single point of contact for AMBER Alert Activations in the Commonwealth, whether responding officers are local officers or Massachusetts State Police members.

AMBER Alert Criteria

AMBER Alerts shall only be activated when:

- A law enforcement officer has determined that a child, seventeen (17) years of age or younger has been abducted;
- The child is believed to be in danger of serious bodily harm or death; and
- There is enough descriptive information to believe an AMBER Alert will help locate the child.

Note: AMBER Alerts are not intended for missing child incidents, runaways, or child custody situations – unless the above three criteria have been met. If these conditions are not met, refer to SOC-04 Lost/Missing Person Searches.

Preliminary Response

Responding local law enforcement or Massachusetts State Police shall be referred/transferred to MSP Operations at GHQ (508-820-2121) during the preliminary investigation of a potential or progressing child abduction scenario that may meet AMBER Alert criteria.

The on-duty MSP Watch Center Lieutenant shall speak with the requesting officer/agency and complete the Massachusetts AMBER Alert Activation Form, then notify the AMBER Alert Activator.

Subject:	Number:
AMBER Alert Activation	**SOC-04A**

Duties & Responsibilities

Position	Responsibilities
First Responding State Police Officer	• Conduct an initial scene assessment to determine if AMBER Alert Criteria has been met; • Verify witness(es) observations to the abduction; • Notify the Desk Officer with specific information and request an immediate AMBER Alert Activation; • Remain at the scene until relieved by a Supervisor; and • Complete an incident report detailing the response.
Desk Officer	• Dispatch the appropriate patrols; • Notify the Troop Duty Officer of jurisdiction with the specific information for an AMBER Alert Activation; • Broadcast pertinent information via the radio; and • Document the Request for an AMBER Alert Activation request from the responding Trooper/Officer into the Daily Administrative Journal (DAJ)/ACISS.
Troop Duty Officer	• When the MSP is the law enforcement agency (LEA) of jurisdiction, contact the MSP Watch Center. **Note:** The Watch Center Officer in Charge (OIC) shall complete the AMBER Alert Activation Form; • Assign a supervisor to respond to the scene, who shall maintain contact with the Troop Duty Officer; and • Advise the Troop Dispatch Center of the pending AMBER Alert request.
Watch Center OIC	• Maintain situational awareness of AMBER Alert activations and potential activations; • Provide relevant information on potential and actual AMBER Alert Activations to Media Relations; • Complete intake process by filling out the AMBER Alert Activation Request form based on information provided by LEA having jurisdiction for all potential AMBER Alert requests; • Notify the AMBER Alert Activator with the specific information received from the AMBER Alert Activation Request Form; • Assist AMBER Alert Activator and facilitate the AMBER Alert request process; • Assist AMBER Alert Activator and investigators with investigative and intelligence support; • Notify the Division Commanders of Field Services, Homeland Security and Investigative Services when an AMBER Alert Activation has been authorized; and • Notify the State Police Detective Unit (SPDU) of jurisdiction on-call officer and the Violent Fugitive

Duties & Responsibilities, continued

	Apprehension Section (VFAS) of jurisdiction on-call officer when an AMBER Alert Activation is pending and/or has been authorized.
MSP Operations at GHQ (Formerly MSP Communication)	• Enter the information into NCIC upon AMBER Alert **activation**, if not already completed by the investigating agency or Troop of jurisdiction; and • Execute the AMBER Alert Activation Checklist at the direction of the AMBER Alert Activator.
AMBER Alert Activator	• Review the Massachusetts Child AMBER Alert Activation Request Form information; • Contact the Troop Duty Officer or requesting LEA if further information is needed to support an activation; • Authorize the AMBER Alert Activation when specific criteria warrant such activation; • Notify the submitting Troop or LEA of jurisdiction when the AMBER Alert Activation is authorized or denied; • Only when an AMBER Alert Activation has been authorized, provide notification to WBZ Radio; • Consider notification to other States, if necessary; • Complete an initial incident report on all activations; and forward the original to the Division Commander of Investigative Services and a copy to the AMBER Alert Program Coordinator; and • Ensure that all relevant notifications are made.
SPDU of Jurisdiction On-Call Officer	• Respond to the scene and conduct an investigation if the Department is the agency of jurisdiction; or • Respond to the scene and act as a liaison between the local LEA of jurisdiction and the AMBER Alert Activator when an AMBER Alert is pending and/or has been authorized.
Violent Fugitive Apprehension Section (VFAS) of Jurisdiction On-Call Officer	• At the request of the AMBER Alert Activator, respond to the scene and provide assistance when an AMBER Alert is pending and/or has been authorized.
Media Relations	• Remain in close contact with AMBER Alert Activator, MSP GHQ Operations and Watch Center OIC to gather accurate developing information relevant facts and circumstances of the potential abduction and potential AMBER Alert Activation, to include the victim, suspect, vehicle, last known location and any other pertinent information;

Duties & Responsibilities, continued

Media Relations, continued	• Once confirmed that a suspected abduction has occurred, and in coordination with the LEA of jurisdiction and the Watch Center OIC (and prior to an MSP decision on potential AMBER activation) release relevant information about the suspected abduction via traditional and social media. This step is undertaken even prior to a decision being made on activation in the interest of expediency, so that members of the public may be alert for sightings of the child/suspect/vehicle at the soonest possible time; • Continue to monitor investigative developments and update traditional media and social media accordingly; • Upon the decision to activate an AMBER Alert, update traditional and social media with information that an AMBER Alert has been officially activated; and • Upon location of the child and/or deactivation of the AMBER Alert, make appropriate updates via traditional and social media.
AMBER Alert Program Coordinator	• Oversee the AMBER Alert Program within the Department; • After any AMBER Alert activation, assemble representatives involved in the activation to coordinate and prepare the after-action report in conjunction with the AMBER Alert Activator; • Submit findings of the after-action report through channels to the office of the Superintendent; • Maintain a database on all activations and after-action reports; • Conduct Program outreach in coordination with Media Relations about the Program; and • Convene the Massachusetts Child AMBER Alert Committee to meet annually as needed.
Director of Telecommunication	• Establish training guidelines for 911 call takers and dispatchers on the Amber Alert plan in consultation with the State 911 Department.
Superintendent	• Assign a Division of Investigative Services Deputy Division Commander, as the AMBER Alert Program Coordinator; and • Assign Commissioned Officers from the Division of Investigative Services, Division of Homeland Security, and Mass State Police Crime Lab (MSPCL) as the AMBER Alert Activators.

Subject:	Number:
AMBER Alert Activation	**SOC-04A**

References: SOC-04 Lost/Missing Person Searches;
National Center for Missing and Exploited Children (NCMEC);
Massachusetts Amber Alert Activation Request Form;
MSP Amber Alert Activation Checklist (Addendum 1);
MPAC: 41.2.6.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

2080

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**SOC-05**
Subject:	
Special Considerations	

Policy

In accordance with international, federal, and state laws, the following are entitled to special considerations and/or immunities:

- Diplomatic and consular officers;
- Foreign Nationals;
- Individuals requesting political asylum;
- Military personnel; and
- Elected officials.

Diplomatic and Consular Officers

Diplomatic Immunity

Diplomatic Immunity is a principle of international law accorded to duly-accredited diplomatic officers, their families, and their servants that afford them qualified exemptions from local jurisdictional prosecution.

Federal law grants members of foreign diplomatic missions and consular posts privileges and immunities in their offices, private residences, as well as in their papers and correspondence.

Members may consult the U. S. Department of State publication ***Diplomatic or Consular Immunity****- Guidance for Law Enforcement and Judicial Authorities* for further information: *https://www.state.gov/wp-content/uploads/2019/09/19-04499-DipConImm v2 web.pdf*

For urgent telephone inquiries outside normal business hours, please call the Diplomatic Security Command Center at 866-217-2089.

Identification

Foreign nationals who enjoy privileges and immunities possess a valid diplomatic passport issued by their country with a diplomatic "A" or "G" visa.

Other formal documents of identity issued by the U.S. State Department includes a (3¾" x 2½") card with photo which depicts:

- Blue border - Diplomatic officers and their families;
- Green border - Embassy administrative and technical staff and their families; or
- Red border - Consular officers, employees and their families.

Vehicle Registration

The State Department has revised the diplomatic and consular license plates. These plates may or may not designate consular or diplomatic codes to correspond to the owner's privileges and immunities.
Members may consult the U. S. Department of State publication ***Diplomatic or Consular Immunity***- *Guidance for Law Enforcement and Judicial Authorities* for further information: *https://www.state.gov/wp-content/uploads/2019/09/19-04499-DipConImm_v2_web.pdf*

Members shall:
Not tow or boot any vehicle bearing a diplomatic or consular license plate, however, the vehicle may be moved to the nearest safe location for reasons of public safety.

Diplomatic Immunity Incidents

The following individuals shall not be detained, handcuffed, or arrested:

- Diplomatic agents or their administrative and technical staff;
- Diplomatic level staff of the United Nations; or
- Family members of any of the above.

Exception: Reasonable restraints may be applied in emergency circumstances involving self-defense, public safety, or the prevention of serious criminal acts.

Incidents involving foreign diplomatic and consular personnel shall be fully documented to assist the State Department in subsequent prosecution or expulsion.

Civil Infractions

No person is exempt from being issued a citation for a civil motor vehicle violation.

Diplomatic Immunity and OUI

If…	Then…
Operating Under the Influence and has a diplomatic "A" or "G" visa.	Sobriety tests may be offered but not compelled. Do not allow the person to drive, however, a member may: • Transport operator to a police station to arrange for safe transport; or • Contact a taxi, friend, or relative of the individual to drive, or assist in making arrangements.

Notifications

When any foreign diplomatic official, members of their family, or staff are involved in any State Police action the Troop Commander shall:

- Immediately notify their Division Commander; and
- Notify the State Department at (202) 895-3682 or call the telephone number listed on the reverse of the subject's identity card issued by the U.S. Department of State, if after regular business hours.

Foreign Nationals

Introductions

The State Department requires assistance from state and local police in carrying out certain international obligations arising from the arrest, detention, or death of foreign nationals (citizens of other countries).

For the purposes of consular notification, foreign nationals include lawful permanent resident aliens of the United States who have a resident alien registration card (commonly known as a "green card").

When foreign nationals are involved in an incident, members shall consult *"Consular Notification and Access"* provided by the Department of State, and are available to all stations via the web site at:

- https://travel.state.gov/content/travel/en/consularnotification.html

International Drivers Licenses

Some foreign nationals, while in the United States, may legally drive using their country's license for up to one (1) year from the person's date of entry into the country, unless they establish permanent residency or employment in this country.

Massachusetts shall only honor valid licenses from countries identified within the current Massachusetts Driver's Manual Appendices:

- *Parties to the Road Traffic Convention and the 1943 Inter-American Automotive Traffic Convention*.

This publication is available to all members via the Massachusetts Registry of Motor Vehicles web site under:

- Forms & Manuals→ Driver's Manual→ Appendices "A".

This also applies to private vehicle registrations, when accompanied by a plaque indicating the country of origin.

An operator with a valid driver's license from Germany or Switzerland shall be considered to be duly licensed to operate in Massachusetts.

Foreign Nationals Arrest or Detention

Position	Duties
Member	• Immediately notify a supervisor of the arrest or detainment of a foreign national.
Supervisor	• Inform the detainee of the detainee's right to have their government notified; • Notify the Troop Duty Officer of the detention and of the notification of the detainee's rights; and • Subject to laws and Department procedures, allow consular officers to visit and converse with the detainee.
Troop Duty Officer	• Notify the Troop Commander; and • If the detainee requests, or if it is mandated, notify the appropriate consulate or embassy without delay, and document the notification.

Mandated Reporting

Agreements with certain countries mandate that they be notified when their nationals are confined or detained regardless of the national's request. These countries are listed in *"Consular Notification and Access"* provided by the Department of State, and are available to all stations via the web site at: https://travel.state.gov/content/dam/travel/CNAtrainingresources/CNA%20Manual%205th%20Edition_September%202018.pdf

Station Commanders shall ensure that the Consular Notification and Access List is updated and available in the guidebook.

Questions

Members who have questions regarding Consular Notification may contact U.S. Department of State at (202) 485-7703 or after regular business hours the Department of State Operations Center at (202) 647-1512.

Ship and Aircraft Incidents

If a ship or aircraft registered in a foreign country crashes within the United States, the nearest consular offices of that country shall be notified immediately.

Deaths of Foreign Nationals

Article 37 of the Vienna Convention on Consular Relations requires that if federal, state or local government officials become aware of the death of a foreign national in the United States, they must ensure that the nearest consulate of that national's country is notified of the death. Members who become aware of such incidents in the course of their duties shall make appropriate notification in a timely manner.

Requests for Political Asylum

Asylum

Asylum is defined as protection and immunity from extradition granted by the United States to a foreign national who is unable or unwilling to return to their country of nationality because of persecution or a well-founded fear of persecution on account of race, religion, nationality, membership in a particular social group, or political opinion.

Request for Asylum

If approached by a foreign national seeking asylum

Step	Action
1	Prevent attempts at forced repatriation, and try to make the person feel comfortable and safe: • Offer protection; and/or • Invite the person to the nearest Department station or facility.
2	Obtain personal data/history: • Name, nationality, date and place of birth, and any documents; • Whether person is alone or with a group; and • Whether person has family, friends, or relatives nearby.
3	Notify a supervisor and the Troop/Section/Unit Commander of the situation.
4	Notify U.S. Immigration and Customs Enforcement (ICE) Boston office (617) 565-3100/3104 to transfer the case.

Elected Officials

National Senators and Congressional Representatives

U.S. Senators and Representatives shall in all cases, except treason, felony, and breach of peace, be privileged from arrest during their attendance at the session of their respective houses, and in going to and returning from the same; and for any speech or debate in either house, they shall not be questioned in any other place. *(U.S. Constitution Article 1, section 6, clause 1.)*

Massachusetts State Senators and State Representatives

No member of the House of Representatives or Senate shall be arrested, or held to bail while going to, returning from, or attending the General Assembly. (Massachusetts Constitution Part 2 C.1 §3 Articles 10 & 11.)

If…	Then…
A Senator or Representative, as outlined above, is en route to an official function associated within the scope of their duties:	• Release forthwith; and • Take action at a later date.
OUI or endangering public safety:	• Normal arrest process.

Elected Officials

Notification

The Troop Commander shall immediately notify the Division Commander and the Office of the Superintendent when any elected or appointed official is arrested or detained for a crime.

Military Personnel

Exceptions To License Requirements

Members shall be aware that Massachusetts General Laws (MGL) c.90, s.5B, s.9B, and s.10 allow several exceptions to license and registration requirements for members of the Armed Forces and their spouses.

References:

MPAC: 1.1.4
MA Constitution - Pt. 2 C.1 §3 Articles 10 & 11;
MGL c.40, §22D;
MGL c.85, §2C;
MGL c.90, §5B, §9B, & §10;
U.S. Constitution Article 1, section 6, clause 1;
22 USC 254 Diplomatic Relations Act;
U.S. Department of State Publication: *"Consular Notification and Access";*
U.S. Department of State Publication: *Diplomatic or Consular Immunity*- Guidance for Law Enforcement and Judicial Authorities;
Massachusetts Registry of Motor Vehicles: *Parties to the Road Traffic Convention and the 1943 Inter-American Automotive Traffic Convention.*

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**SOC-06**

Subject:

Administration of Naloxone Hydrochloride (Narcan)

Policy

This policy shall establish protocol for Department members in order to reduce life-threatening emergencies of fatal opioid overdoses, where medical professionals are not readily available, by administering naloxone hydrochloride.

Department members shall assist any person who may be suffering from an opioid overdose. Department members trained in accordance with this policy shall make every reasonable effort, to include the use of naloxone combined with First Responder Training, to revive the victim of any apparent drug overdose.

Definitions

Mucosal Atomization Device: Used to deliver a mist of atomized medication that is absorbed through the nasal mucosa into a person's blood stream and into the brain and cerebrospinal fluid.

Naloxone Hydrochloride or Narcan: An opioid receptor antagonist and antidote for opioid overdose administered in intramuscular, intranasal or intravenous forms. The intranasal form, using prefilled syringes compatible with Mucosal Atomization Device, is permitted for use by first responders under Massachusetts Office of Emergency Medical Services Statewide Protocol Standing Orders.

Opioids: Medication that reduces the intensity of pain signals to the brain and affects those brain areas controlling mood, memory, reward and emotion, which diminishe the effects of a painful stimulus, but also can result in addiction. Opioids at high doses reduce the drive to breathe, which can result in inadequate oxygen to the brain and overdose. Medications that fall within this class include hydrocodone, oxycodone, morphine, codeine, and related drugs e.g., heroin potent illicit derived from morphine that is prohibited for medical use in the United States.

Subject: Dispensing of Naloxone Hydrochloride (Narcan)	Number: SOC-06

Definitions, continued

Opioid Overdose: An acute condition including, but not limited to, decreased level of consciousness, respiratory depression, coma, or death resulting from the consumption of an opioid, or another substance with which an opioid was combined, or that a layperson would reasonably believe to be an opioid-related drug overdose that requires medical assistance.

Universal Precautions: An approach to infection control to treat all human blood and certain human body fluids as if they were known to be infectious for HIV, HBV and other blood borne pathogens.

Training

Department members issued Naloxone Hydrochloride (Narcan), shall:

- Be trained by the Department's Medical Unit on responding to persons suffering from an apparent opioid overdose and the use of Narcan; and
- Receive refresher training every two (2) years that may be done in conjunction with First Aid/CPR Training.

Training shall follow recommendations from the Office of Emergency Medical Services (EMS) - Department of Public Health, *Administrative Requirements Manual AR-2-100* as amended.

Issue of Narcan

Department members who are authorized shall:

- Carry a Narcan kit with a Mucosal Atomization Device according to EMS Statewide Treatment Protocols;
- Follow Narcan and First Responder training conducted by the Department's Medical Unit;
- Store their Narcan kit with their first aid kits, however, during extreme hot and cold temperatures or when on extended leave, Narcan kits should be removed from vehicles and maintained at room temperature (59-86 degree F) away from direct sunlight;
- Report missing, damaged or expired Narcan kits to their immediate supervisor;
- Dispose of MAD syringes and Narcan vials in a biohazard sharps container; and
- Request replacement Narcan kits through channels to the Department's Medical Unit.

Subject: Dispensing of Naloxone Hydrochloride (Narcan)	Number: SOC-06

Issue of Narcan, continued

Immediate Supervisors shall:

- Document in writing any reports of missing, damaged or expired Narcan kits; and
- Forward the documentation through channels to their Division Commander's Office for further action in coordination with the Officer-In-Charge (OIC) of the State Police Medical Unit.

Use of Narcan

When dispensing Narcan Department members shall:

- Maintain universal precautions;
- Follow training received from the Department's Medical Unit on protocols and procedures for the administration of Narcan;
- Ensure SP 900 Naloxone Hydrochloride (Narcan) Administration Incident Record is completed for each Narcan administration and forward through channels to the Department's Medical Unit.

Medical Unit

The Department's Medical Unit shall:

- Ensure Department members receive training in the dispensing of Narcan according to EMS and the Statewide Treatment Protocols;
- Authorize and supply members with Narcan kits as needed;
- Ensure SP 900 Naloxone Hydrochloride (Narcan) Administration Incident Record is forwarded to the identified Medical Director of the Naloxone Hydrochloride (Narcan) Program; and
- Keep training records of all Department members authorized to dispense Narcan.

References:

105 Code of Massachusetts Regulations (CMR) 171.165;
105 Code of Massachusetts Regulations (CMR) 700.003;
SP 900 Incident Report for the Administration of Naloxone Hydrochloride (Narcan);
Office of Emergency Medical Services(EMS)- Department of Public Health: *Administrative Requirements Manual AR-2-100 (3/27/2014).*

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**SOC-07**
Subject:	
Domestic Abuse	

Policy

The Department shall adhere to the Massachusetts Domestic Violence Law Enforcement Guidelines 2001.

Definitions

Abuse: For the purposes of this policy, abuse is defined by Massachusetts General Laws (MGL) c.209A, §1 as the occurrence of one or more of the following acts between family or household members:

- Attempting to cause or causing physical harm;
- Placing another in fear of imminent serious physical harm; or
- Causing another to engage involuntarily in sexual relations by force, threat, or duress.

Family or Household Members: Persons who:

- Are or were married to one another;
- Are or were residing together in the same household;
- Are or were related by blood or marriage;
- Have a child in common regardless of whether they have ever married or lived together; or
- Are or have been in a substantive dating or engagement relationship, including same sex relationships.

Response

Domestic abuse situations are considered a high priority and require that members immediately respond to the scene. Notifications shall be made to the department of jurisdiction as appropriate with an offer made of Department assistance.

The State Police Detective Unit (SPDU) of jurisdiction shall be notified of all domestic abuse cases involving serious bodily injury or injury which results in a death.

Response, continued

Position	Duties
Desk Officer/ Dispatcher	• Whenever possible, two (2) members should be dispatched to the scene; o Provide available information as requested: o Provide information about the existence of any warrants or protective orders, or record of criminal history; o Provide any other relevant information of prior incidents or likelihood of firearms being present; and o Provide any record of Firearms Identification Cards and/or Licenses To Carry Firearms issued to resident(s); and • Notify the Troop Duty Officer. Note: A response shall not be terminated based on a follow-up call from the complainant.
Responding Member(s)	Whenever there is reason to believe that a family or household member has been abused, or is in danger of being abused, members shall: • Arrest the abuser where probable cause exists; • Request medical treatment if appropriate; • Activate the Emergency Judicial Response System (EJR); • Remain on the scene; • Immediately provide the abuse victim with copy of a SP 500 Abused Persons Notice of Rights; • Assist victim and dependent children to a safe place; • Provide referral information for programs, shelters, and counseling to victims; and • Inform victim that abuser may be eligible for bail.

Supervisor Responsibilities

Supervisors shall ensure the provisions of MGL c.209A, as well as these guidelines, are adhered to:

- That an incident report has been filed, even in cases where no arrest was made; and
- That calls which are received as allegations of domestic abuse or a domestic disturbance are not reclassified because no probable cause to arrest existed. Incident reports shall be filed in those cases as well.

Supervisor Responsibilities, continued

If upon review of an incident report, it is believed that probable cause exists, the supervisor shall:

- If required, ensure that a follow-up investigation is conducted;
- Ascertain that appropriate referrals are provided to the victim; and
- Ensure that criminal charges are initiated according to MGL c.209A.

Notice of Rights

The investigating member shall immediate provide abuse victims with adequate notice of rights. The notice shall consist of:

- Handing the victim a copy of SP 500; and
- Reading the victim their rights.

When the victim's native language is not English, every attempt shall be made to provide the statement in their native language.

Confidentiality

A plaintiff's residential address and workplace address shall appear on the court order and be accessible to the defendant unless the plaintiff specifically requests that this information be withheld from the order.

Members assisting in emergency abuse prevention orders shall be cognizant of victims' confidentiality rights and requests.

Service of Orders

Service of orders shall be made in hand, unless otherwise ordered by the court. Orders shall be:

- Served promptly upon receipt. If service is initially unsuccessful, the Department shall continue to attempt service until it is completed. Service of orders shall not be delayed in order to be served by a specialized officer or unit; and
- Returned to the court promptly.

The victim's safety shall be considered in the timing of the service of the order. Members should encourage the victim to contact an advocate (either through the District Attorney's (DA) Office of jurisdiction, SAFEPLAN, or the local battered women's program) in order to develop a safety plan around the service of the order.

Troop/Station/Section/Unit Commanders shall maintain a record of all attempts at service.

Out of State Orders

Persons who violate out of state abuse orders, or violate Massachusetts abuse orders in another state, may be charged criminally for contempt in the Commonwealth of Massachusetts.

- In assessing probable cause, a member may presume the validity of the protection order issued by another jurisdiction when the member has been provided with:
  - A copy of the order by any source; and
  - A statement by the victim that such order remains in effect.

A protective order issued in another jurisdiction (as defined in MGL c.209A, §1) shall be given full faith and credit in the Commonwealth. Therefore, members shall make a warrantless arrest of any person, when the member has probable cause to believe there is a violation of an emergency, temporary or permanent vacate, refrain from abuse, stay away or no-contact order, or judgment issued by another jurisdiction.

Firearms

In domestic abuse incidents, members shall seize all firearms in accordance with SOC-07A Domestic Abuse Arrest/Investigations.

Vacate Orders and Court Orders to Retrieve Belongings

Once a vacate, no contact, stay away, or refrain from abuse order is issued, members shall not accompany any party to the property without specific judicial authorization. A vacate order may include the following requirement:

- The defendant shall not damage any of the plaintiff's belongings, or those of another occupant, and shall not interfere with any utilities or mail delivery to the plaintiff.

The defendant in the vacate order may be allowed to retrieve their belongings under the following conditions and shall:

- Have a court order allowing for the retrieval; and
- Not be allowed to use this as a means of harassing the victim.

The victim/defendant shall have prior notice by the Department, and shall agree to the timing of the retrieval.

Note: Members need to keep in mind that certain behaviors by the victim or the defendant, while at the residence, may constitute a violation of the protective order. Repeated visits may also constitute a violation. The purpose of the restraining order is to keep the defendant away from the plaintiff. If the defendant repeatedly returns to collect their belongings, it is defeating the purpose of the protective order.

Vacate Orders and Court Orders to Retrieve Belongings, continued

In cases where one party has a court order that allows them to return to a residence in order to retrieve their belongings, members shall:

- Accompany the victim to ensure the order is executed: and
- Ensure the victim is free from harassment or abuse by the defendant.

Referral Information

Troop/Station/Section/Unit Commanders shall ensure that referral information for programs, shelters, and counseling for victims are identified within their respective jurisdictions and available within the guidebook.

Confidential Programs Locations

A domestic abuse program is defined as any refuge, shelter, office, safe home, institution, or center established for the purpose of offering assistance to victims of abuse through crisis intervention, medical, legal, or support counseling.

The location and street address of all domestic abuse programs are absolutely confidential and shall not be revealed in any criminal or civil proceeding.

Under no circumstances shall law enforcement officers release information to anyone, other than another law enforcement officer or a victim, regarding the location of a domestic abuse program.

References:

SOC-07A Domestic Abuse Arrest/Investigations;
SP 500Abused Person's Notice of Rights;
Massachusetts Domestic Violence Law Enforcement Guidelines 2001 (Revised);
Chapter 164 of the Acts of 2000: An Act Relative to the Crime of Criminal Harassment;
MGL c.209A, 8, as amended by c.236 s.24 of the Acts of 2000;
MGL c.209A;
MGL c.233, §20K;
MGL c.233, §20L;
MGL c.265, §43 Stalking;
MGL c.277, §62B Stalking; jurisdiction.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**SOC-07A**
Subject:	
Domestic Abuse Arrest/Investigations	

Policy

The Department shall respond and investigate allegations of domestic abuse while ensuring the rights and safety of all those involved.

Arrest Guidelines

The safety of the victim and any children shall be paramount in any decision to arrest, and in the timing of the arrest. The decision to arrest shall be based on whether or not probable cause exists that a crime occurred, not on whether or not the victim wishes to seek complaints or wishes to testify at a future date.

Mandatory Arrest: Members shall make a warrantless arrest of any person the member witnesses or has probable cause to believe has violated an emergency, temporary or permanent vacate, refrain from abuse, stay away or no-contact order, or a judgment, suspension, surrender and/or a protection order issued by any jurisdiction.

Arrest Preferred: When there are no refrain from abuse, vacate, stay-away, or no-contact orders or judgments in effect, arrest shall be the preferred response whenever a member witnesses or has probable cause to believe that a person has committed:

- A felony;
- An assault and battery of a family or household member in violation of Massachusetts General Laws (MGL) c.265, §13A;
- A misdemeanor involving abuse, as defined in MGL c.209A;
- An assault and battery or permits another to commit an assault and battery upon an elder or a person with a disability in violation of MGL c.265, §13K;
- An assault and battery with or without a dangerous weapon on an individual under the protection of an abuse prevention order, as defined in MGL c.265 §13A(b)(iii) and 15A(c)(iii); or
- An assault on an individual who is known to be pregnant, or there is reason to know is pregnant.

Arrest Guidelines, continued

When probable cause to arrest exists and the suspect has fled the scene, the member shall:

- Have the Desk Officer/Dispatcher advise area patrols and all local police departments as appropriate;
- Attempt to make a warrantless arrest; and
- Seek an arrest warrant from the appropriate court, as soon as possible.

A statement from a police department that probable cause to arrest exists shall be honored by another police department. When probable cause exists to believe a crime involving abuse occurred, members shall not advise the victim to seek complaint applications on their own.

Investigations

Members responding to domestic abuse calls shall follow the guidelines established in SOC-07 Domestic Abuse and ensure an investigation includes:

- Information about the suspect's ownership, access to, or presence of any firearms, and their location;
- Relationships of all parties at the scene, including names and DOB of children present, or those in the household;
- The phone number of the victim’s residence and include the number within the incident report so the bail bondsman or court personnel may inform the victim of the defendant’s release on bail; and
- Informing the victim that if they intend to leave the residence, and desire to be informed of the abuser’s release on bail, they must provide a contact number.

Members shall be aware that thorough documentation of the crime scene condition is critical to the prosecution.

Defendant Information

Members shall provide information regarding a defendant's dangerousness to the Prosecutor for use at arraignment such as:

- Criminal history;
- Restraining, no-contact or other protective orders currently in effect against the suspect;
- Possession of, or past use of weapons;
- Threats of serious physical harm against the victim, other family members, or pets; or
- Attempts or threats to commit suicide.

Arrest of a Caretaker

In cases involving abuse of a child**,** a person with a disability, or an elder, members shall:

- Address the issue of whether or not the victim can be left alone safely, if the abuser is arrested; and
- Contact the respective protective agency in order to arrange for temporary care, if the child, person with a disability, or the elder cannot be left alone.

In situations involving allegations of abuse of children, the disabled, or the elderly refer to SOC-07C Abuse of Children/Disabled/Elderly.

Substantive Dating Relationship

Members shall gather enough information to determine whether or not a substantive dating relationship exists and examine the following factors when making this determination:

- The length of time of the relationship;
- The type of relationship;
- The frequency of interaction between the parties; and
- If the relationship has been terminated by either person, the length of time that has elapsed since the termination of the relationship.

If it is determined that a substantive dating relationship exists or did exist, then the member shall:

- Take proper action, including arrest when appropriate, regardless of whether the victim seeks a restraining order.

In cases where there is no substantive dating relationship, another crime such as stalking or criminal harassment may have been committed.

Dual Arrests

Dual arrests, like the issuance of mutual restraining orders, are strongly discouraged because they trivialize the seriousness of domestic abuse and increase the danger to victims. In the majority of cases, an effective investigation will reveal the dominant aggressor. Members shall:

- Attempt to identify the dominant aggressor bearing in mind the difference between offensive and self-defense injuries; and
- Take action based on that determination.

A member arresting both parties is required by law to submit separate and detailed arrest reports indicating the basis for the dual arrest.

Members investigating an incident of domestic violence shall not discourage requests for law enforcement intervention by threatening, or otherwise indicating all parties will be arrested.

Incident Reports

Incident reports shall be made whether or not an arrest results. Upon request to the Department, reports shall be made available to the victim at no cost. Prosecution and subsequent legal action can be greatly aided by documentation and description of:

- Physical injuries; and
- Photographs of the injuries.

Members shall note the presence of children in the household and other information gained through the investigation.

Confidentiality

The Department shall ensure the confidentiality of domestic abuse victims by safe guarding certain information including, but not limited to:

- Information regarding the identity of a victim or children;
- Any medical information;
- Statement by witnesses; or
- Keeping a separate record of the victim's home and work address and phone numbers if the victim will be seeking to hide from the abuser.

Victims of domestic abuse have a strong privacy interest in this type of information whether contained in the initial incident report or supplemental reports. Domestic abuse reports shall only be released to the victim and the District Attorney's Office of jurisdiction. Any other requests for a domestic abuse report shall be forwarded to the Department's Legal Section.

Firearms

Firearms at the scene of a domestic abuse incident.

If…	Then…
The responding members are informed that a firearm or weapon has been involved in the dispute.	• Seize the weapon as evidence of the crime.
The weapon is not reported to have been involved in the dispute.	• Request that the firearm or weapon be placed in the Department's custody temporarily.

A consent search is permitted by law in all jointly controlled or accessible areas. Members shall:

- Take temporary custody of the firearm or weapon to alleviate the threat of serious violence; and
- Ascertain whether a firearm is lawfully possessed.

Firearms, continued

If the member determines that the weapon cannot be seized, then:

- A judge can order the defendant to surrender all firearms, and their Licenses To Carry (LTC) Firearms including their Firearms Identification Card (FID); or
- The issuing authority may revoke or suspend the LTC or FID, which would then allow for the seizure of the firearms.

In all domestic abuse cases, the investigating member shall advise the licensing authority that the subject of the license is suspected of abuse. Notice may be made by mailing or faxing a copy of the incident report to the local licensing authority after authorization from the Department's Legal Section.

Abuse Prevention Orders

Upon issuance of any order under MGL c.209A Abuse Prevention Orders, *that specifically mandates that all firearms be surrendered*, members shall:

- Immediately take possession of all firearms, rifles, shotguns, machine guns, and ammunition, including any LTC and FID, owned or controlled by the subject of the order; and
- Ensure that the court order has been completely vacated prior to returning weapons and permits.

Violations of Orders

In the interest of immediacy and the statutory mandate to arrest, members shall:

- Make a warrantless arrest of any person the member witnesses or has probable cause to believe has violated an order, including a violation which stems from the possession of weapons.

Seizure and Storage of Firearms

Every department within the Commonwealth shall honor another department's request for assistance in seizing the above listed items regardless of which department is named within the order. The department named within the order shall be responsible for the storage of the seized items or the delegation of storage to an authorized facility.

Orders Against Law Enforcement Officers

In cases involving police officers that are defendants in Abuse Prevention Orders which require the surrender of all firearms**,** the defendant must relinquish all firearms, including departmental weapons, to the department serving the order.

Federal Firearms Provisions

The Colonel/Superintendent shall be notified whenever a member identifies a case involving certain circumstances of which federal action can be taken. Members shall be cognizant of the following federal provisions:

Persons Named in Protective Orders
Under the Federal Crime Control and Law Enforcement Act of 1994, it is unlawful for an individual subject to a permanent restraining order involving intimate partners to receive, ship, transport, or possess guns (including handguns, rifles, and shotguns) or ammunition, that traveled through interstate commerce.

Misdemeanors Involving Domestic Violence
Under 18 USC § 922(g)(9), it is unlawful for any person convicted of certain misdemeanor crimes involving domestic violence to ship, transport, possess, sells, or otherwise dispose of, or receive firearms or ammunition.

Federal Felon in Possession Of A Firearm
Under 18 USC § 922(g)(1), "Felon in possession of a firearm," it is unlawful for any person who has been convicted in any court of a crime punishable by imprisonment for a term exceeding one year to possess any gun or ammunition.

Property

The relationship of the parties and their property interests complicate domestic abuse situations. When a party to a domestic dispute is accused of removing, or attempting to remove property from the dwelling, or is accused of damaging or destroying property, the member shall:

- Conduct an investigation to determine the civil or criminal consequences; and
- Take appropriate action if criminal (e.g. malicious destruction of property).

Police Officers from Other Jurisdictions

In cases involving police officers from other jurisdictions, the investigation shall follow the guidelines established within this policy and SOC-07. The supervisor shall:

- Immediately notify the OIC of the employing department;
- Ensure information is entered into the RAMS system and/or ACISS, the Daily Administrative Journal and other appropriate reports;
- Secure the local weapon until returned to the involved Department; and
- Forward a copy of the report to the Chief of Police of the involved officer, through the Department’s Legal Section

Subject:	Number:
Domestic Abuse Arrest/Investigations	**SOC-07A**

References: SOC-07 Domestic Abuse;
SOC-07B Domestic Abuse Involving MSP Members;
SOC-07C Abuse of Children/Disabled/Elderly;
MGL c.209A, § 6(7);
MGL c.265, § 13A;
MGL c.265, § 13K;
MGL c.265, § 15A.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

2101

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**SOC-07B**
Subject:	
Domestic Abuse Involving Members	

Policy

The Department shall ensure that all reports of alleged domestic abuse by members are thoroughly investigated.

The Department shall respond and investigate allegations of domestic abuse while ensuring the rights and safety of all those involved.

Involved Member

Any member, upon being notified that they are a defendant in any protective order or modification thereof, or upon becoming aware that they have been accused of abuse, shall:

- Immediately notify their duty assignment supervisor (pursuant to Rules and Regulations), naming the investigating department, if any;
- Surrender Department issued License To Carry (LTC) Firearms and/or weapons and any other state or federal firearms licenses to the responding supervisor; and
- Within twenty-four (24) hours, make written notification, through channels, to their Division Commander. A copy of the protective order or modification shall also be attached to the documentation.

Responding Member

All members responding to incidents of alleged domestic abuse involving members of the Department shall:

- Take immediate action to ensure the safety of the victim;
- Call a supervisor of higher rank than the involved member to the scene;
- Remain on the scene until relieved by the responding supervisor;
- Ensure that all provisions of Massachusetts General Laws (MGL) 209A are followed, including arrest, when necessary; and
- Submit a detailed report of observations and statements made, prior to the end of their shift.

Responding Supervisor

Whenever a member is alleged to have committed abuse, a supervisor of higher rank than the accused member shall be assigned to conduct a criminal investigation. When a protective order is issued, or when the supervisor has reason to believe that the member committed abuse, the supervisor shall immediately:

- Relieve the accused member from duty;
- Seize all Department issued use of force weapons, pursuant to Departmental Rules and Regulations;
- Seize all other firearms and/or weapons at the scene;
- Seize member's LTC, and any other state or federal firearms licenses;
- Notify the member's Troop/Section Commander;
- Seize Department issued vehicle and conduct a vehicle inventory;
- Identify outstanding protective orders against the accused member;
- Ensure that all provisions of MGL 209A are followed, including arrest and further investigation, when appropriate;
- Forward LTC and any other state or federal firearms licenses to the Administrative Investigator;
- Complete an incident report prior to the end of their shift and forward to the Troop/Section Commander; and
- Ensure the complaint has been documented in a To/From format and fax to the Division of Standards and Training (DST) prior to the end of their shift.

Division Commander's Responsibilities

When an abuse prevention order is issued, or when there is reason to believe that the member committed abuse, the Division Commander shall:

- Assign a Commissioned/Staff Officer to conduct an administrative investigation;
- Immediately ensure that the accused member is or has been relieved from duty pursuant to Departmental Rules and Regulations;
- Convene a Duty Status Hearing, pursuant to Department Rules and Regulations; and
- Review reports and initiate additional investigations as necessary.

Administrative Investigation

In all incidents where a member has been accused of abuse, a thorough administrative investigation shall be conducted by a Commissioned/Staff Officer, preferably of higher rank than that of the accused member. The investigation shall include, but not be limited to the following:

- Identify all outstanding and expired protective orders against the accused member;
- Collect and review all reports, affidavits, and records pertaining to the allegations of abuse; and
- Interview the victim and other witnesses.

Administrative Investigation, continued

Other duties of the Administrative Investigator include:

- Working with the criminal investigator (if any) to ensure that the provisions of MGL 209A are adhered to, including criminal action or arrest when appropriate;
- Ensuring appropriate referral information has been given to the victim regarding battered women's programs, emergency shelter, counseling services, and court based advocacy services;
- Forwarding all available documents to the Duty Status Board;
- Attending all court proceedings and maintaining contact with any assigned prosecutor or probation officer; and
- Forwarding copies of all reports to the Internal Affairs Section upon completion of the investigation.

Division of Standards and Training

In domestic abuse cases involving Staff Officers, the DST Commander shall notify the Colonel/ Superintendent.

Complaint Notification to DST

In addition to any other required reports, all complaints of domestic abuse involving members shall be documented and submitted to the Division of Standards and Training (DST).

Member	Action
Member Receiving Complaint	**Internal Complaints** Internal personnel complaints originating within the Department, shall: • Be documented in a To/From format; • Faxed to the Division of Standards and Training within twenty-four (24) hours from the date of the To/From; • Submit a copy through channels to the appropriate Troop/Section/Unit Commander; and • Forward the original copy to the Division of Standards and Training.
Administrative Investigation	The Commissioned/Staff Officer conducting the administrative investigation shall: • Document the complaint in a To/From: • Fax to DST at 508-820-2149 within 24 hours of receipt; • Forward a copy through channels to the appropriate Troop/Section/Unit Commander; and • Forward the original to DST.

Subject: Domestic Abuse Involving Members	Number: SOC-07B

References: ADM-14 Personnel Investigation;
SOC-07 Domestic Abuse;
SOC-07A Domestic Abuse Arrest/Investigations;
SOC-07C Abuse of Children/Disabled/Elderly;
Rules and Regulations;
SPAM Collective Bargaining Agreement Article 27.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

2105

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**SOC-07C**
Subject:	
Abuse of Children/Disabled/Elderly	

Policy

The Department shall investigate all allegations regarding the abuse of children, the disabled, and the elderly, to ensure the safety and rights of all those involved.

Mandated Reporting

Investigating members shall make mandated reports by immediately contacting the designated agency with an immediate oral report, and shall submit a report in writing **within forty-eight (48) hours** after the initial oral report. Members shall contact:

- Department of Children and Families (DCF) whenever they have reasonable cause to believe that a child under the age of eighteen (18) has been abused or neglected. The member shall:
  - Call to make an oral report Monday-Friday during the hours of 9:00 A.M. to 5:00 P.M. to the nearest DCF Office found at the bottom of the revised DCF form *"Report of Child(ren) Alleged to be Suffering from Serious Physical or Emotional Injury by Abuse or Neglect"*; or
  - Call to make an oral report after 5:00 P.M. Monday-Friday and twenty-four (24) hours on weekends and holidays to the Child-At-Risk-Hotline 1-800-792-5200; and
  - Submit the written report by either by mail, email or fax within forty-eight (48) hours to DCF. To assist in the written notification of child abuse/neglect, DCF has establish a form *"Report of Child(ren) Alleged to be Suffering from Serious Physical or Emotional Injury by Abuse or Neglect"*. This form can be obtained from DocuShare under Bulletins or from the DCF website: www.mass.gov/dcf .
- Disabled Persons Protection Commission whenever they have reasonable cause to believe that a caretaker has abused/neglected a disabled person, between the ages of eighteen (18) and fifty-nine (59). At any time call (800) 426-9009.
- Executive Office of Elder Affairs whenever they have reasonable cause to believe that someone age sixty (60) or older has been abused/neglected. At any time call (800) 922-2275.

Subject:	Number:
Abuse of Children/Disabled/Elderly	**SOC-07C**

Notifications

Troop Duty Officers shall notify the State Police Detective Unit of jurisdiction in cases where abuse of children, the disabled, and/or the elderly involve serious bodily injury or results in death.

Arrest of a Caretaker

In cases involving abuse of a child, a disabled person, or an elderly person, members shall:

- Address the issue of whether or not the victim can be left alone safely, if the abuser is arrested; and
- Contact the respective protective agency in order to arrange for temporary care, if the child, the disabled person, or the elderly person cannot be left alone.

References:

SOC-07 Domestic Abuse;
SOC-07A Domestic Abuse Arrest/Investigations;
SOC-07B Domestic Abuse Involving MSP Members;
MGL c.119, s.51A;
MGL c.19C, s.10;
MGL c.19A, s.14-26;
Department of Children and Families (DCF) *"Report of Child(ren) Alleged to be Suffering from Serious Physical or Emotional Injury by Abuse or Neglect"*.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Policy Date:	Number:
July 22, 2022	**SOC-08**
Subject:	
Missing/Abandoned/Runaway Children	

Policy

The Department shall thoroughly investigate all reports of missing children. Every child reported missing to the Department will be considered at risk until significant information to the contrary is confirmed. Incidents involving missing, abandoned and/or a runaway child shall be treated as a potential emergency event that may require a rapid and coordinated response of specialized personnel and equipment. Every lost and/or missing child incident has the potential of being or becoming a criminal investigation; members shall treat the scene of each incident as a potential crime scene.

Jurisdictional conflicts are to be avoided when a child is reported missing. Questions concerning parental custody occasionally arise in relation to missing-child reports. It shall be the policy of this agency to accept the report of a missing child even if custody has not been formally established. The safety of the missing child(ren) is paramount, members will initiate an investigation when it can be shown the child has been removed, without explanation, from their last known location. If custody has not been established by the Court, then the law-enforcement responsibility is to ensure the child is safe only.

If the missing child is identified as being age seventeen (17) or younger and there is evidence of abduction, the Amber Alert Coordinator shall be notified.

Definitions

Abandoned: A child whose parents or guardians abscond from their legal responsibilities to care for their child. – MGL c. 119 §39.
Note: Does NOT include newborn infants, 7 days of age, or less, that are voluntarily placed with a hospital, police department or manned fire station. – MGL c. 119 §39 ½ "Baby Safe Haven Act"

Juvenile: A child who has not attained their 18th birthday. May also be referred to as "child" for purposes of this policy.

Lost, Injured or Otherwise Missing: A child who has disappeared under unknown circumstances.

Runaway: A child, often a teenager, who leaves home voluntarily for a variety of reasons.

Definitions, continued

Thrownaway: A child whose caretaker makes no effort to recover the child after running away, has been abandoned or deserted, or who has been asked to leave their home and not allowed to return.

Zone of Safety: National Center for Missing and Exploited Children state that the zone of safety for a child will vary depending on the age of the child and their developmental stage. In the case of an infant, for example, the zone of safety will include the immediate presence of an adult custodian or the crib, stroller, or carriage in which the infant was placed. For a school-aged child the zone of safety might be the immediate neighborhood or route taken between home and school.

Risk Factors and Response

A missing child will be considered at risk when the below factors are present:

- Not attained their 14th birthday; AND/OR
- Believed or determined to be experiencing one or more of the below circumstances:
  - Is out of the zone of safety for their age and developmental stage;
  - Has identified cognitive challenges;
  - Is drug dependent, including prescribed medication and / or illegal substances;
  - Has been absent from home for more than 24 hours prior to notification of law enforcement;
  - Is in a potentially life threatening situation;
  - May be in the company of other identified individuals who may be engaged in behavior(s) that may-endanger the child's welfare;
  - Is absent in a way inconsistent with the established patterns of behavior and the deviation cannot be readily explained; and/or
  - Is involved in a situation causing a reasonable person to conclude the child should be considered at risk.

The presence of risk factors, or other extenuating information, involved in the report of a missing child will qualify as a child at risk and an expanded investigation, including the use of all appropriate resources, will immediately commence.

If appropriate, existing interagency response protocols – including the AMBER Alert system and / or other immediate community notification methods, if available – should be considered.

Subject: Missing/Abandoned/Runaway Children	Number: SOC-08

Responsibilities

Position	Duties
Desk Officer / Dispatcher	The Desk Officer or designee, including but not limited to the dispatcher, should conduct the following upon receiving a report of a missing child. • Determine if circumstances of the report meet the definition of a missing child; • Dispatch a member to the scene of the report; • Notify the Duty Officer; • Transmit a description of the child over the Troop radio system; • Notify the local police department of jurisdiction. o Ascertain if the local police department of jurisdiction is in need of State Police assistance. o Record the request or declining of State Police services in the Daily Administrative Journal (DAJ) and advise responding member(s); o Notify the Troop Duty Officer of the notification and subsequent local police department acceptance or declination of services. o Provide assistance as requested by the local law enforcement agency. • Search Department RMS systems and other records management for related information, specifically any records such as those pertaining to the family, the place where the child was last seen, and the child's residence; • Safeguard all pertinent records in accordance with record retention regulations and investigative needs; • Activate established protocols for working with the media – including activation of the AMBER Alert system and / or other immediate community notification methods when appropriate; and • Make appropriate entries in the DAJ.

Responsibilities, continued

Position	Duties
Responding Member(s)	• Respond promptly to the scene; • Interview the parent(s) or person who made the initial report; • Obtain a detailed description of the missing child including recent photo(s) and/or video(s). • Complete the SP-622 Lost / Missing Person Questionnaire; • Confirm the child is in fact missing; • Verify the child's custody status; • Identify the circumstances of the missing episode; • Make an initial assessment of the type of incident; • Identify the missing child's zone of safety for their age and developmental stage; • Inquire if the child has access to the Internet, cell phone, and / or other communications device; • Conduct an immediate, thorough search of the scene. Refer to SOC-04 Lost / Missing Person Searches; • Determine when, where, and by whom the missing child was last seen; • Interview the individual(s) who last had contact with the missing child; • Identify and separately interview everyone at the scene; • Obtain a description of the suspected abductor(s) if applicable, and other pertinent information; • Determine the correct NCIC Missing Person File category and ensure notification is promptly entered; • Provide detailed descriptive information to the Troop Dispatcher for broadcast updates; • Seal / protect scene, area of child's home, and areas of interest as potential crime scenes; and • Prepare necessary reports and complete appropriate forms. o Responding members shall complete an incident report. o The Department of Children and Families (DCF) shall be notified; and • Should the incident indicate abuse or neglect, a 51a shall be filed.

Responsibilities, continued

Position	Duties
Troop Duty Officer	• Assign a supervisor to respond to the scene; • Make appropriate DAJ entries and SAM notification as warranted; • Notify the Troop Commander if the child is not immediately located; • Assist in the activation of the AMBER Alert system as requested; • Notify the State Police Detective Unit (SPDU) if appropriate; • Coordinate between partner agencies and deploy resources as needed; and • Notify Media Relations.
Supervisor Responsibilities	• Obtain a briefing and written reports from the first responder(s) and other agency personnel at the scene; • Determine if additional personnel and resources are needed to assist in the investigation; • Initiate activation of the Amber Alert System if warranted; • Initiate immediate community notification methods, such as reverse 911 notification system(s); • Establish a command post and other ICS protocols; • Organize and coordinate search efforts; • Ensure all required notifications have been made; and • Ensure the child is entered into NCIS as missing.
Division of Investigative Services	• When warranted, and upon request, the SPDU of jurisdiction shall meet with the investigating member(s) and initiate or assist with an investigation of the circumstances surrounding the missing child. If such investigation is initiated, the SPDU of jurisdiction shall communicate relevant information to the initiating investigating member(s).

Unidentified Persons

A member assigned to the report of an unidentified person, whether living or deceased, who appears to be a child, shall:

- Obtain a complete description;
- Enter the unidentified child's description into the NCIC Unidentified Person File;
- Use all available resources to aid in the identification of the child; and
- Cancel all notifications after identification is confirmed.

Recovery or Return of Missing Child

A member assigned to the recovery or return of a missing child shall:

- Verify the located child is, in fact, the reported missing child;
- Secure intervention services, if appropriate;
- Arrange the return of the child to their legal guardian or an appropriate children's shelter in the case of a runaway or missing child who has been located and who is not wanted on a warrant or other law violation;
- In the case of a runaway from another jurisdiction who has been located and a warrant exists or an NCIC missing-person "hit" is verified, place the child in custody and transport them to the appropriate facility for admission; and
- Notify DCF and the local police department of jurisdiction of the recovery/return.

Safe Haven Exception

In accordance with MGL Chapter 119 § 39½, in the event a parent voluntarily abandons an infant 7 days of age or less at any MSP facility, a member will:

- Immediately take custody of the newborn;
- Notify EMS and have the infant transported to the hospital to be evaluated;
- Follow EMS to the hospital and ensure that DCF is notified of such abandonment;
- Enter all appropriate information into the DAJ; and
- Complete an incident report.

If the infant shows signs of abuse, the Member is required to submit a 51A form under MGL Chapter 119. (Voluntary abandonment of an infant shall not by itself constitute either a finding of abuse or neglect or a violation of criminal law.)

Safe Haven Exception, continued

The Member accepting a newborn infant will make every effort to solicit the following information from the parents leaving the newborn infant:

- Name of newborn infant;
- Name and address of parent placing the newborn infant;
- Birthplace of newborn infant;
- Information relative to newborn infant's medical history and their biological family's medical history if available;
- Any other information that might reasonably assist DCF or the court in current or future determinations of the best interests of the child; and
- Whether parent plans on returning to seek future custody of infant.

The Member receiving the newborn infant will encourage the parent to provide the information but the parent will not be required to provide such information.

References

SOC-04 Lost / Missing Person Searches;
SOC-04A Amber Alert Activations;
SP-622 Lost / Missing Person Questionnaire;
MGL c119 §39 and c119 §39 ½;
MPAC: 41.2.6.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**SOC-09**

Subject:

Terrorism/WMD Incidents

Policy

The preservation of life and the prevention of injury shall be recognized as high priorities in responding to terrorist incidents, including those involving Weapons of Mass Destruction.

Terrorism

Terrorism is the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

WMD

Weapons of Mass Destruction (WMD) can be chemical, biological, radiological, nuclear or explosive (CBRNE) weapons that have potential for creating mass casualty incidents.

SP 2810 Form

All Members shall keep a copy of the SP 2810 Crime Scene Threat Assessment Worksheet folded inside the Emergency Response Guidebook in their cruiser. Copies of SP 2810 shall be maintained at each Department facility or within the Emergency Response Guidebook to be accessible to Desk Officers and Troop Duty Officers.

Responding Members

When ...	Then ...
Responding to routine calls for service:	• Respond with due caution; callers may lack a complete understanding of the situation and may not convey the existence of on-scene hazards.
There is the potential that a terrorist or WMD event is occurring:	• Ensure the safety of all responders and the public; and • When possible, review SP 2810 and relay pertinent information to the Desk Officer.

Subject:	Number:
Terrorism/WMD Incidents	**SOC-09**

Responding Members, continued

When ...	Then ...
Relaying information from the SP 2810:	• Utilize the most secure channel of communication at your immediate disposal; and • If it is necessary to relay information via radio, request a Code 1.
On-scene hazards threaten life or health:	• The preservation of life and the prevention of injury shall be of the highest priority.
Members inadvertently encounter a potentially contaminated area:	• Avoid contact; • Minimize exposure; • Never purposefully touch, taste or smell any object, package, or container, etc.; • Warn others; • If possible, isolate area; and • Stay upwind and uphill.
Issues arise concerning the crime scene or the securing of evidence:	• Contact the Troop Duty Officer for guidance.

Desk Officer

If ...	Then ...
A report is received involving a potential terrorist or WMD event:	• Transmit the most detailed information possible to all responding members; and • Relay all available information from the scene to the Troop Duty Officer, assigned patrols, local police, and fire departments.
A report is received involving a potential terrorist or WMD event:	• Relay all available information from the scene to GHQ Communications and the Troop Commander (who shall contact the Division Commander); • Contact the local fire department to activate Department of Fire Services-Regional Hazardous Materials Team (877)385-0822; • Contact the Department State Police Detective Unit (SPDU) of jurisdiction; and • Ensure that the area hospitals are advised.

Troop Duty Officer

If ...	Then ...
The incident involves a suspected explosive device or a suspicious package:	• Contact the Bomb Squad; and • Refer to SOC-02 Bomb Threat/Explosives Incidents.
The incident involves a hazardous material:	• Contact the local fire department to activate Department of Fire Services-Regional Hazardous Materials Team (877)385-0822; and • Refer to SOC-01 Hazardous Materials.
Issues arise concerning the crime scene or the securing of evidence:	• Contact the SPDU of jurisdiction; and • The Division of Investigative Services (DIS) representative shall be designated the officer-in-charge.

GHQ Communications Section

If ...	Then ...
A report is received involving a potential terrorist or WMD event:	In addition to duties required by other written directives, the GHQ Communications Section shall notify: • The Office of the Superintendent; • The Division of Investigative Services and Field Services Commanders; • Media Relations; • The Commonwealth Fusion Center; • Massachusetts Emergency Management Agency (MEMA); and • Department of Fire Services-Regional Hazardous Materials Team; and • The National Guard Civil Support Team, if needed.
The incident involves a suspected explosive device or a suspicious package:	• Contact the Bomb Squad; and • Refer to SOC-02 Bomb Threat/ Explosives Incidents.

Subject:	Number:
Terrorism/WMD Incidents	**SOC-09**

GHQ Communications Section, continued

If ...	Then ...
The incident involves a hazardous material:	• Contact the local fire department to activate Department of Fire Services-Regional Hazardous Materials Team (877)385-0822; and • Refer to SOC-01 Hazardous Materials.

DIS

If…	Then…
A preliminary investigation into a reported potential terrorist or WMD event reveals a hoax or an unsubstantiated incident:	• The Division of Investigative Services shall prepare an after action report within forty-eight (48) hours in order to make use of "lessons learned."

References: SOC-01 Hazardous Materials;
SOC-02 Bomb Threat/ Explosives Incidents;
SP 2810 Crime Scene Threat Assessment Worksheet;
U.S. Department of Transportation Emergency Response Guidebook.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

2118

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**SOC-10**
Subject:	
Clandestine Drug Laboratory Response	

Policy

The Department recognizes the inherent dangers of clandestine drug laboratories and sets forth the following procedures to be followed by all Department members. These procedures are in compliance with Federal Occupational Safety and Health Administration (OSHA) Standards and are designed to limit dangers to Department members and the public.

Purpose

To define the role of the Clandestine Laboratory Enforcement Team (CLET) and establish guidelines for the utilization and activation of team members.

Definitions

Clandestine Lab (Clan Lab): The operation at any location consisting of chemicals, mixtures, or processes designed or intended to synthesize, extract or convert illegal or controlled substances to include but not be limited to:

- Methamphetamine, Ecstasy, LSD, Fentanyl, THC and other illegal drugs.

Clandestine Laboratory Enforcement Team (CLET): A multi-agency team of law enforcement officers and certified chemists who have completed the Drug Enforcement Agency (DEA) Basic Clandestine Laboratory Certification School.

Site Safety Officer: A CLET member who has completed the DEA Advanced Site Safety School. The Site Safety Officer is responsible for the safe operation and adherence to DEA procedures at clan lab sites.

Utilization of CLET

CLET is available when requested to assist members from the Department and those from other local, state, and federal agencies for:

- Known or suspected clan labs or their investigations;
- Execution of search warrants at clan lab locations;
- Training personnel relative to clan labs; and
- Other special events as assigned by the Commander of the Division of Investigative Services or designee.

Subject: Clandestine Drug Laboratory Response	Number: SOC-10

CLET Activation Protocol

Requests for CLET services shall be made to the Troop Duty Officer and shall include:

- The name, rank, and agency name of the requesting officer;
- The name of the primary point of contact and a call-back number;
- The nature of the request; and
- The exact location of the incident and any designated staging areas.

The Troop Duty Officer shall contact:

- the Department's CLET Leader, or designee; and
- the on-call member of the State Police Detective Unit of jurisdiction.

The CLET Leader, or designee, shall:

- Assess the situation;
- Activate the necessary Department's CLET members, to include the Department's chemists, and
- Contact the DEA CLET Coordinator.

Note: The CLET Leader shall maintain the current list of certified CLET members.

Activation/ Contact Number

During business hours: contact MSP Fire and Explosion Investigation Unit (978)567-3310.

After business hours: contact Troop Duty Office.

Authority

No member of the Department shall enter a known/suspected clan lab site unless:

- Authorized by a CLET Site Safety Officer; or
- Imminent or immediate danger exists to others.

CLET members shall assume complete control and authority of all identified clan lab sites.

While engaged in clan lab operations, CLET members shall take direct orders only from the:

- CLET Leader or designee;
- Site Safety Officer;
- DEA Clan Lab Coordinator;
- Division of Investigative Services Commander or designee; or
- Colonel/Superintendent.

Operational Protocols

Department Members

Department members who discover or are advised of a suspected clan lab shall:

- Immediately notify the Troop Duty Office;
- **NOT** attempt to touch, turn off, adjust or otherwise manipulate any switches, controls or other materials within the suspected clan lab;
- Secure the area around the suspected clan lab and remain at a safe distance from the lab; and
- Remain on the scene until properly relieved.

CLET Leader

The CLET Leader, or designee, after assessing the situation, shall determine the need for additional resources including, but not limited to:

- Local Fire Department(s);
- MSP Bomb Squad;
- Department of Fire Services Hazardous Materials Team;
- Emergency Medical Services (EMS); and
- Traffic mitigation and controls.

CLET Members

CLET members shall:

- Assist and advise on-scene Incident Commander by recommending actions, coordinating resources, and/or providing appropriate documentation related to an on-going incident; and
- Provide assistance by coordinating internal or external agency resources that can be utilized to respond, mitigate, and/or recover from an incident in accordance with Incident Command System (ICS) protocols.

The Site Safety Officer shall coordinate and work with Department and CLET members from other agencies to respond to mitigate and recover Clandestine Drug Laboratory scenes in accordance with CLET Standard Operating Procedure (SOP).

Evidence Considerations

The collection of evidence, contraband and materials shall be coordinated by CLET members in consultation with chemists (either state or federal).

The Department member or local officer who is the case officer shall ensure evidence preservation and custody.

Subject: Clandestine Drug Laboratory Response	Number: SOC-10

After Action Reporting

Following the completion of any critical incident, CLET members shall conduct a debriefing.

The CLET Leader, the Site Safety Officer, or designee, is responsible for the completion of any after action reports or CLET reporting as applicable. After Action Reports shall be forwarded to the Division of Investigative Services Commander or designee for review.

References: 29 CFR 1910.120 Occupational Safety and Health Administration Standard.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

2122

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**SUP-01**
Subject:	
Jurisdiction/Mutual Aid	

Policy

The Department shall ensure that its members are informed of the limits of their police authority and shall work in cooperation with other law enforcement agencies.

Jurisdiction

The Department has sole and/or concurrent jurisdiction within the territorial boundaries of the Commonwealth.

Limits on Jurisdiction

No member may be used or called upon for service at any industrial dispute unless actual violence has occurred therein, and then only by written order of the Governor.

Members shall not exercise police powers on a reservation or other property of the United States of America unless requested by the person in charge of the reservation or property.

Members have no police powers in any Massachusetts Correctional Institution (MCI) facility, except by direction of the principal officer.

New England State Police Administrators Compact

The Commonwealth of Massachusetts has entered into a mutual aid agreement with State Police agencies in adjoining states. The agreement, known as the New England State Police Administrators Compact (NESPAC), provides for:

- Cooperation and assistance in detecting and apprehending those engaged in criminal activity;
- Establishing and maintaining an information sharing system to be accessed by participatory agencies;
- Mutual aid and assistance in the event of police emergencies; and
- The granting of powers, duties, rights, privileges, and immunities of police personnel when rendering such aid.

Subject:	Number:
Jurisdiction/Mutual Aid	**SUP-01**

Requests for Mutual Aid

When approved by the Colonel/Superintendent, Department personnel or other resources may be provided at no cost to other law enforcement agencies.

When any other law enforcement agency requests mutual aid from the Department, the initial request should contain:

- Nature and duration of the request;
- Contact information for requesting department's officer-in-charge (OIC); and
- Expenditures, if any, which shall be borne by the requesting agency.

The Troop/Section/Unit Commander or designee shall be responsible for determining which personnel shall be dispatched to the incident while maintaining adequate Department services within their command.

Requests by the Department

In the event of an unusual, natural, or man-made emergency situation, the Colonel/Superintendent shall request authorization from the Executive Office of Public Safety and Security:

- To seek assistance from any appropriate state/federal agency;
- To seek assistance from the Massachusetts National Guard; and
- To grant personnel from outside the Department powers as a State Police Officer.

State of Emergency

Upon declaration of a "State of Emergency" by the Governor, all members (excluding personnel on suspension, injury, or other approved leaves) shall immediately contact their duty assignment supervisor, or other supervising officer within their chain-of-command, for specific instructions.

After Action Reporting

The Commanding Officer/OIC rendering assistance shall make a complete and accurate accounting which shall include, at a minimum:

- Number/names of members assigned, and time expended;
- Specific action taken; and
- Equipment utilized.

Subject:	Number:
Jurisdiction/Mutual Aid	**SUP-01**

After Action Reporting, continued

The Colonel/Superintendent may require a Division Commander or a Troop Commander to complete an After Action Report on significant incidents to determine if:

- Established Rules & Regulations, Policies & Procedures, orders and directives were followed;
- Available resources (personnel, equipment, etc.) were utilized in the most effective and efficient manner possible;
- Whether there is any deficiency or inadequacy in training, supervision, or policy which needs correction, enhancement, or adoption; and
- Conclusion(s), opinion(s), and recommendation(s).

References: MPAC 2.1.1, 2.1.2, 2.1.3, 2.1.4.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

2125

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**SUP-03**
Subject:	
Media Relations	

Policy

The Department shall provide the media and the public with information on Department operations and administration while ensuring that individual rights are protected.

On-scene supervisor(s) of incidents with a large scale media presence shall establish a media staging area to facilitate effective communication through Media Relations who shall be the primary point of contact and dissemination of information between the Department and media organizations.

Employees assigned to Media Relations shall receive proper training of the basic guidelines, skills and knowledge needed to capably perform the duties of a Law Enforcement Public Information Officer.

Dissemination of Information

Employees shall treat official business of the Department as confidential. Information shall only be disseminated according to established procedures. Employees shall not:

- Disseminate information in violation of Rules and Regulations*;* or
- Disseminate information prohibited by this policy; or
- Disseminate information prohibited by federal or state law, or a court order.

Driver's Privacy Act

The release of information obtained through any state motor vehicle database shall not be released to non-law enforcement personnel.

Significant News or Events

The Office of the Colonel/Superintendent or Media Relations shall be the authorized source for the dissemination of all press releases.

When a member is involved in an incident or significant event that may be considered of interest to the public, the member or the Desk Officer shall contact Media Relations to provide the necessary information.

Examples of such incidents or events may include, but are not necessarily limited to:

- A significant arrest or investigation;
- Search or rescue;
- Motor vehicle crash with fatal or life-threatening injuries;
- Large scale Department law enforcement operations, or

- Incidents involving the Department and other public service agencies involved in a mutual effort.

Any inquiries from the media about such types of incidents shall be referred to Media Relations.

Media Relations

Troop/Section/Unit Commanders shall assist Media Relations with:

- Coordinating news conferences;
- Preparing and conducting news releases in the absence of a Media Relations member; and
- Positive news stories involving the Department.

Information for Dissemination

Information generally appropriate for members to disclose to the media and the public includes:

- Typical crash information:
  - Names of the occupants involved, if over eighteen (18) years of age;
  - Cause of crash if known; and
  - Degree of injuries- minor, serious, or no injuries occurred. Note: Do not give out specific injuries of any occupant due to privacy rights.
- Road and weather information;
- Information from the public log (except for prohibited information as outlined within this policy);
- The time and place of arrest;
- An arrested adult's name, age, town, charges and bail status; and
- The name and rank of the investigating and arresting members (except for undercover officers), assisting agencies and the length of the investigation.

Division/Troop/Section Commanders shall:

- Approve, coordinate and/or release information concerning confidential investigations, operations, and emergency/crisis situations to Media Relations.

It is preferred that the Office of the Attorney General (AGO), District Attorney (DA) Offices, the Office of the State Fire Marshal (OSFM), or other outside agencies generate news releases regarding a crime or arrest of concern to that specific office, in coordination with Media Relations, when members of the Department are involved.

Members assigned to the AGO, DA, OSFM, or other agencies shall:

- Not become unilaterally involved in media relations efforts unless approved by the Office of the Colonel/Superintendent or Media Relations.

If the AGO, DA, OSFM, or other agencies choose not to make a news release, Media Relations may do so when authorized by the Office of the Superintendent.

Media Interviews

Media interviews shall be conducted by the highest ranking or most experienced member on-duty in the order of:

- Media Relations;
- Troop/Section/Unit Commander;
- Troop/Section/Unit Duty Officer; or
- A Supervisor, with training or experience in giving interviews.

Note: Troopers shall not be compelled to do television or radio interviews against their wishes.

After consultation with Media Relations personnel, members may give limited interviews:

- To accredited news personnel at the scene of a vehicle crash or criminal incident, if there is no interference to the ongoing investigation; or
- Concerning information regarding road and weather conditions.

Members shall wear the uniform of the day, including the appropriate cover. Members working in a plain clothes assignment shall be appropriately dressed.

All other interviews shall be approved/coordinated through Media Relations.

Prohibited Information For Release

Employees **shall not** release or give out information on:

- The prior criminal records or driver's history of a person, or the existence or nonexistence of a prior criminal record except:
  - To other federal, state, or municipal law enforcement agencies as authorized by the Criminal Offender Record Information (CORI) laws; or
  - To warn the public of imminent danger from such a person; or
  - In connection with serious or violent offenses, to expedite the location and apprehension of such a person.
- The identity of a deceased victim before confirmation has been received that the next of kin has been notified according to ADM-13 Notification of Medical Examiner and/or Next of Kin;
- Information related to victims of domestic abuse in accordance with SOC-07A Domestic Abuse Arrest/Investigations;
- The name or address of a juvenile (refer to INV-05 Juvenile Operations for definition) who is a suspect, defendant, complainant, or victim;
- The name or biographical information of the victim of a sexual crime;
- The name or photograph of an undercover officer;
- The existence or contents of any confession, admission, or statement given by a suspect, however, it may be stated that the defendant denies the charges. Note: This does not apply to statements made by the defendant to representatives of the news media or general public;

- Opinions about the guilt, innocence, character, or reputation of a suspect;

Prohibited Information For Release, continued

- Statements predicting or influencing the outcome of the trial;
- The results, refusal, or failure to submit to any examinations or tests;
- Statements or opinions concerning the credibility or testimony of prospective witnesses;
- Information that may adversely affect an investigation or prosecution of a case;
- Information about ongoing litigation;
- Any medical information;
- Causes of death until officially determined by the Medical Examiner;
- Disabled individuals per MGL c.41 §98F; or
- Other information as outlined in the Rules and Regulations.

Photographs

The news media may photograph a person in custody. However, members shall not:

- Pose prisoners for news photographs;
- Allow prisoners to be photographed in Department facilities; or
- Allow prisoners to be photographed in other facilities against the wishes of the owner.

Members should not interfere with photographing or televising of a defendant in a public area, unless such activities:

- Interferes with their official duties; or
- Violate a court order.

Media Relations shall be contacted:

- Before the release of any photograph of Department employees; and
- Before the release of any photograph of a suspect or defendant.
  Note: Members shall be mindful that booking photos may be considered part of a subject's CORI record and the release of these photos must be approved by MSP Legal.

The release of photographs of Department undercover officers shall only be approved by the Colonel/Superintendent or the Deputy Superintendent.

Access to Crime And Crash Scenes

Representatives of the news media shall not be permitted to interfere with investigations or the efficient flow of traffic. However, news media representatives may be:

- Granted access to crime or emergency scenes; and
- Allowed to locate their vehicles and equipment at points nearer to a scene than permitted by normal traffic.

Subject: Media Relations	Number: SUP-03

Access to Crime And Crash Scenes, continued

Permission for media access to a scene occurring in a private dwelling or other area generally not open to the public shall:

- Be obtained from lawful authority over the premises including government entities, such as the Turnpike or Port Authority; and
- Be controlled by a supervisor in command of the scene ensuring the particular needs of the investigation take precedence.

Note: Most accredited news reporters and photographers have identification cards that are issued by their respective employer.

References:
ADM-13 Notification of Medical Examiner and/or Next of Kin;
INV-05 Juvenile Operations;
MGL c.6, §167-178;
MGL c.41, §98F;
18 USC 2722 Driver's Privacy Protection Act;
MPAC: 54.1.3, 54.1.4 .

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**SUP-04**
Subject:	
Employee Assistance Unit	

Policy

The Department has a responsibility to ensure the safety of our employees and to contribute to their psychological and physical well-being. The Department shall offer to its employees and their families, professional assistance, training, peer counselling, and professional referrals as needed and requested. These same services are available to other state, county, and local law enforcement agencies and their families.

Availability

The Employee Assistance Unit (EAU) is available (24) hours a day by calling (978) 975-0794 or the GHQ Communications Section at (508) 820-2121. The EAU is available to:

- All Department employees and family members; and
- State, County, and Local law enforcement agencies and their families.

Members of the EAU are available:

- To meet employees, members of other agencies, and their families who request assistance at a mutually acceptable time and location;
- To provide telephone support to those listed above;
- To provide training to recruit training classes;
- To provide specialized training upon request; and
- To oversee training and credentialing of, and coordinate responses by, MSP Peers for Critical Incident Stress Management (CISM) responses.

Responsibility

Employee Assistance Unit members shall:

- Not represent themselves to any third party as the Department's agent for purposes of adjudication, placement or disposition; and
- Not be held responsible for decisions made by any employee receiving EAU services that prove to be in violation of Department rules, regulations, policies, or procedures.

In no event shall a member's involvement with the Employee Assistance Program abrogate their responsibility to conform or comply with rules, regulations, policies and procedures.

Accordingly, and in furtherance of EAU's commitment to recovery and good health, EAU members shall:

- Remind anyone receiving such services that compliance with rules, regulations, policies, and procedures must remain a primary factor in all personal decisions.

Subject: Employee Assistance Unit	Number: SUP-04

Confidentiality

It is critical for the success of the Employee Assistance program that confidentiality of case information be maintained. The members assigned to the EAU shall ensure that information obtained from an employee, member of another agency, or their families remains confidential, **unless failure to disclose such information could cause a clear and present danger to the safety or security of an individual, the public, or the Department**.

Members of the EAU, as part of the Massachusetts State Peer Support Network and working within the umbrella of the MSP EAU, operate with privileged communication under MGL. c. 233, § 20O.

Reports

Written and oral reports shall contain only that information that is pertinent to an ongoing evaluation.

Every effort shall be made to avoid any undue invasion of privacy.

Procedure

Supervisors should remain alert for signs of unhealthy stress in their employees, particularly when involved in a highly traumatic incident. Reactions to stress may appear immediately after an incident; however, they may not appear for hours, days, or even weeks later.

Supervisors should notify the EAU as soon as possible, but no later than eighteen (18) hours following occurrences of:

- Critical incidents that may evoke extraordinary emotion;
- On or off duty death, serious injury, or serious illness of an employee or family member;
- Unusual death or violence to a child, or a victim known by an employee;
- Use of force incidents involving death or serious injury;
- Fatal accidents involving Department vehicles, or pursuits;
- A prolonged rescue situation that ends in failure;
- When an employee's work performance appears to be affected by stress; or
- Any time a supervisor believes that the employee may benefit from EAU assistance

In any highly traumatic incident where an employee is affected, or is likely to be affected, supervisors should:

- Assign a support employee, preferably a friend, to the employee for close contact;
- When possible, assign the employee to a role within the incident where there is a decreased risk of unnecessarily traumatizing the employee;
- Isolate and remove the employee from the scene of the incident, if needed and operationally possible;

Subject: Employee Assistance Unit	Number: SUP-04

Procedure, continued

- Ensure against unnecessary repetition of statements and accounts of the incident by the affected employee;
- Assist the employee in preparing the official report; and
- Monitor the employee's condition closely over the following weeks and months for signs of unhealthy stress.

Employees may be referred to the EAU when they may not be aware of the adverse impact of an event on them, or suppress the need for emotional/psychological care.

Administrative Leave/ Temporary Modified Duty

Any employee directly involved in a high-risk situation that may adversely affect personal or professional conduct may be placed on Administrative Leave or Administrative Duty by the Colonel/Superintendent. EAU should be notified when a sworn member is to be relieved of duty and when practicable, accompany the member's supervisor who is affecting relief. This reassignment shall be clearly noted to the employee as not being punitive in any way.

The EAU may recommend members for placement on Temporary Modified Duty as approved by the Colonel/Superintendent. This is a management action used to deal with stress for the individual and the organization, and allows the member to refocus and cope with the situation in a healthy and positive manner.

Commanding Officers shall consult with the EAU prior to the employee resuming regular duties.

References: ADM-18 Anti-Harassment/Sexual Harassment and Discrimination;
MGL c.112, §134, s.135, § 135A, § 135B;
MGL c. 233, § 20O.
Bernard v. Commonwealth, 424 Mass. 32 (1996).

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
February 17, 2023	**SUP-04A**

Subject:

Critical Incident Stress Management Team

Policy

The CISM Team is managed by the Employee Assistance Unit. Members of the Critical Incident Stress Management Team will be volunteers who are and remain in good standing with the Department.

The Department will determine the number of personnel assigned to the CISM Team. As needed, the Department will publish an open announcement requesting interested candidates apply to become a member of the CISM Team. Selections to the Team will be at the discretion of the Department.

CISM Team member activity shall be monitored and approved by the Employee Assistance Unit (EAU) Commander and/or designee. When services are requested and approved, CISM Team members shall assist members from other local, state, and federal first responder agencies.

The EAU Commander or designee shall utilize a CISM Team and provide direction to that team in a manner consistent with the International Critical Incident Stress Foundation (ICISF) guidelines.

The CISM Team shall maintain membership with the Massachusetts State Peer Support Network (MSPSN).

CISM Team members agree to resign from the Team at the request of the EAU Unit Commander

Purpose

To establish and define the role of the Critical Incident Stress Management (CISM) Team within the Department and establish guidelines for activation and utilization of its resources.

To lessen the impact of a critical incident and enhance the coping abilities of involved members through emotional and tangible support, with the goal of maintaining employee wellness and operational readiness.

Definitions

Critical Incident: For purposes of this General Order, a critical incident is defined as an event resulting in psychological stress or trauma to an emergency service provider because of an emergency service provider's response to an incident. A critical incident is further defined as an incident that necessitates an EAU response and a member is in need of peer support (e.g., serious motor vehicle crash, a serious injury or fatality involving a civilian, death or serious injury of a member, officer involved shooting, severe trauma or death of a child, and mass casualty event).

Critical Incident Stress Management Team members: Department sworn members and non-sworn members from all ranks and Divisions shall be trained and certified in CISM under the ICISF guidelines and consistent with MSPSN requirements. MSP CISM Team members are not counselors or therapists but serve as a peer support network. MSP CISM Team members work as CISM members secondary to their primary assignment within the Department.

Utilization of Resources

Any Department employee shall have the right to access CISM services and request CISM support from a Team member with whom they are comfortable. In such case, CISM Team member shall notify EAU Commander or designee of such request and services rendered.

Operational Protocols

CISM Team members shall:

- Be a "Certified Emergency Service Provider" as defined by M.G.L. Ch. 329 Of the Acts of 2018: "*An Act Relative to Critical Incident Intervention by Emergency Service Providers."*
- Respond to a critical incident or provide peer support when authorized by the EAU Commander or designee.
- Not self-deploy to an incident, however, if the CISM Team member is already on scene or becomes involved and identifies a need to provide services, they shall provide the necessary services and notify the EAU Commander or designee as soon as practicable.
- Be appropriately dressed to be on scene and equipped with proper issued protective gear.
- Respond to a designated staging area and report to CISM Team Commander or their designee.
- Recognize and refer to the EAU, cases that are beyond their scope of training.

Confidentiality

All interactions by MSP CISM Team members with Department personnel during any type of intervention shall be kept strictly confidential.

References: M.G.L. Ch. 329 Of the Acts of 2018: "*An Act Relative to Critical Incident Intervention by Emergency Service Providers*;"
SUP-04: Employee Assistance Unit.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Orders

Effective Date:	Number:
May 25, 2023	**SUP-05**

Subject:

State Police Chaplain Corps

Policy

The State Police Chaplain Corps:

- Is a voluntary support service;
- May assist, but is not intended to replace or impede, the efforts of the Department's Employee Assistance Unit (EAU) and/or the Office of the Ombudsman; and
- Shall provide non-denominational spiritual support and counseling as sought, regardless of gender, gender identity, sexual orientation, race, ethnicity, religious preference, affiliation, or beliefs.

All members of the State Police Chaplain Corps shall take and affirm an Oath of Office prior to the initial performance of duties.

Purpose

To establish guidelines for the responsibilities, organization, and qualifications of chaplains assigned to the Massachusetts State Police Chaplain Corps.

Oath of Office

I solemnly promise that I will faithfully and diligently perform the duties of Police Chaplain for the Department of the Massachusetts State Police, and that I will provide ministry to the officers of the department and to the citizens of the community as I am called upon.

I will strive to set an exemplary standard of ethical and moral conduct and not use my position of Police Chaplain to proselytize or to gain personal advantage and will minister to all persons without religious or other bias.

I will acknowledge those appointed in a position of authority within the department and will serve them with loyalty, and will be supportive of the officers with whom I serve and will be subject to their authority when on duty and will accept the responsibility willingly and without reservation, so help me God.

Requests for Service

The Office of Superintendent shall:

- Coordinate requests for services of the State Police Chaplain Corps with the Director of the State Police Chaplain Corps.

Administrative and Programmatic Oversight

Administrative oversight shall:

- Be conducted by a Commissioned Officer assigned to the Office of the Superintendent.

Programmatic oversight shall:

- Be conducted by the Commanding Officer of the EAU or designee.

Availability

The State Police Chaplain Corps provides services that are available twenty-four (24) hours a day for Department employees when seeking guidance and comfort or at times of illness, injury, or death.

The Department Chaplains may be contacted through the:

- Communications Center at 508-820-2121;
- Department Telephone Directory;
- The EAU; or
- The Ombudsman.

State Police Chaplains shall respond to a critical incident or crime scene when:

- Officially notified by the Department; and
- Render services to only those employees requesting such service.

Upon arriving at a scene, State Police Chaplains shall:

- Immediately identify themselves as a State Police Chaplain, and display the issued Department Identification Card to Officer-In-Charge (OIC) or designee;
- Only enter an active scene when prior approval has been granted from the OIC or designee; and
- As soon as practicable, notify the Commanding Officer of EAU or designee as to such response.

Subject: State Police Chaplain Corps	Number: SUP-05

Responsibilities

State Police Chaplains shall be available to provide support and guidance to Department employees. Their duties shall include, but not be limited to:

- Visits to injured or hospitalized personnel;
- Participation at funeral services;
- Provision of counseling at the request of an employee;
- Assistance in making serious injury or death notifications upon request of the Department;
- Maintenance of strict confidentiality of all Department matters;
- Provision of follow-up assistance to employees of the Department at times of crisis; and
- Participation in Department functions as requested, (i.e. promotional ceremonies, award ceremonies, etc.).

Designation

The Colonel/Superintendent may designate individuals as State Police Chaplains and shall determine the appropriate number of chaplains.

State Police Chaplains shall serve at the discretion of the Colonel/Superintendent on a voluntary basis and shall not receive compensation.

The Colonel/Superintendent shall designate a Chaplain as Director of the Chaplain Corps to oversee the duties and responsibilities of assigned State Police Chaplains and the program.

Qualifications

Qualifications for State Police Chaplains are:

- Affiliation with a recognized, organized religion;
- Demonstration of sufficient experience in community pastoral and parish work;
- Possession of a Bachelor of Arts and Masters of Divinity degree from an accredited college or seminary;
- Possession of a valid Massachusetts Driver's License and access to a properly registered and insured motor vehicle;
- Successful completion of a background investigation (no individual with a past criminal conviction for any offense shall be designated a Department Chaplain); and
- Attend training(s) as required by the Commanding Officer of EAU.

Director of the Chaplain Corps

The Director of the State Police Chaplain Corps shall:

- Coordinate and monitor the activities of the Chaplain Corps; and
- Conduct bi-annual meetings to share information, discuss goals and objectives, and other issues of interest.

Subject:	Number:
State Police Chaplain Corps	**SUP-05**

References: Department of State Police Rules and Regulations.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**SUP-06**
Subject:	
Binding Written Agreements	

Policy

All Memorandum of Understandings, Mutual Aid Agreements, or any other type of binding written agreements (collectively referred to as "MOUs") between the Department and outside organizations, including any state or federal agency, shall only be authorized and signed by the Colonel/Superintendent.

MOU Process

Position	Responsibilities
Troop/Section/Unit Commander	• Carefully review the MOU; and • If approved, forward to their Division Commander.
Division Commander	• Review the forwarded MOU; • Either approve the MOU or recommend changes to the language or terms; • Forward the approved MOU to the Chief Administrative Officer; and • Be responsible for the MOU oversight and renewal.
Chief Administrative Officer	• Review the forwarded MOU; • If need be, return the MOU and supporting documentation to the Division Commander with any recommendations; • Forward a copy of any MOU that pertains to a grant program to the Fiscal Grants Manager and the Strategic Planning Section; and • Forward the approved MOU to the Chief Legal Counsel.

MOU Process, continued

Position	Responsibilities
Chief Legal Counsel	• Review the forwarded MOU; • Submit the reviewed MOU with any recommendations to the Colonel/ Superintendent; • If approved by the Colonel/ Superintendent forward the MOU to the outside agency for signature; • Return a copy of the approved and signed MOU package to the Division Commander and Chief Administrative Officer; and • Retain all signed original MOU documentation for archives.
Colonel/ Superintendent	• Approve all MOUs involving the Department; and • Return signed MOUs to the Chief Legal Counsel.

Written Agreement Sign-Off Sheet

The SP 480 Written Agreement Sign-Off Sheet shall be:

- Attached to all MOU's;
- Submitted through channels; and
- Signed off by all appropriate employees prior to signature by the Colonel/Superintendent.

Property Inventory

Commanding Officers shall ensure that any property acquired as the result of an MOU shall be inventoried and treated in accordance with ADM-30 Asset Management.

Control and Authority

All MOUs for Department law enforcement services shall clearly identify the nature and extent of services to be provided and shall stipulate that the Colonel/Superintendent maintains control and authority over all Department personnel including, but not limited to:

- Hiring;
- Discipline;
- Transfers;
- Promotions;
- Assignments;
- Training; and
- Dismissal.

Subject:	Number:
Binding Written Agreements	**SUP-06**

Services Provided	All MOUs shall include provisions for services provided, but not limited to: • Training; • Equipment; • Facilities; • Functions and activities to be performed; and • Duties and responsibilities.
Financing and Budget	Fiscal accounting shall be clearly articulated to avoid confusion and misunderstandings and shall include, but not be limited to the following: • Salaries, indirect costs, and fringe benefits; • Training and equipment costs; • Maintenance of cost accounting records; • Issuance of fiscal reports; • Time and manner of payment for services; and • Procedures for the disposition of revenues generated by Department law enforcement activity.
Records	MOUs shall specify the types of records required, the frequency of reporting, and the means for maintaining them.
Duration	All MOUs shall include: • Effective beginning and termination dates or conditions; • Procedures for modification or amendment; and • Procedures for termination, if necessary.
Employee Rights	Participation in any MOU shall not penalize the rights of any Department employee.

References: ADM-30 Asset Management;
ADM-47 Grant Approval Process;
SP 480 Written Agreement Sign-Off Sheet.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**SUP-12**
Subject:	
Office of the Ombudsman	

Policy

The Ombudsman Program provides a confidential, neutral, and informal process to help resolve work-related issues. It is a dispute resolution system that offers employees formal and informal options for addressing work-related problems and concerns. Although the program is an alternative channel of communication, it is designed to complement, not replace or circumvent the Department's formal resolution options.

Definitions

Confidential Communications: Communications, or a source of communication, which are intended to be held in secret.

Privileged Communications: Communications that occur in a context of legal or other recognized professional confidentiality.

Office of the Ombudsman

The Office of the Ombudsman reports to the Colonel/Superintendent. The primary role of an Ombudsman is to act as a designated neutral in order to facilitate fair and equitable resolutions regarding work-related problems and concerns.

An Ombudsman shall:

- Attempt to provide informal conciliation, when appropriate;
- Not use the names of individuals without their permission;
- Exercise discretion on whether to act upon a concern of an employee;
- Maintain objectivity and impartiality; and
- Keep professionally current and competent in areas that relate to the role of an Ombudsman and the practices of the Department.

The Ombudsman shall attempt to identify options within the Department to resolve issues brought forth. This includes creating innovative solutions, when possible, or referring individuals to other available Department processes.

Availability

An employee may contact an Ombudsman and leave a confidential voice message at 508-988-7025.

Subject: Office of the Ombudsman	Number: SUP-12

Responsibility

An Ombudsman shall:

- Not represent themselves to any third party as the Department's agent for purposes of adjudication, placement or disposition; and
- Not be held responsible for decisions made by any employee receiving Ombudsman services that prove to be in violation of Department rules, regulations, policies, or procedures.

In no event shall a member's involvement with an Ombudsman abrogate their responsibility to conform or comply with rules, regulations, policies and procedures.

Accordingly, and in furtherance of an Ombudsman commitment to recovery and good health, Ombudsman shall:

- Remind anyone receiving such services that compliance with rules, regulations, policies, and procedures must remain a primary factor in all personal decisions.

Confidentiality

Communications with the Office of the Ombudsman are considered privileged. That privilege cannot be waived, **unless failure to disclose information that was obtained from an employee could cause a clear and present danger to the safety or security of any individual, the public, or the Department.**

Complaints and Department Investigations

The Ombudsman has the responsibility to consider the concerns and rights to privacy of all parties potentially involved in a dispute. The Ombudsman does not take action on calls, letters, or other communications that are anonymous.
However, the Department shall be notified of any alleged criminal conduct committed by an employee.

No acts of reprisal or retaliation shall be tolerated against any employee of the Department as a result of contact with the Office of the Ombudsman.

Records

The Office of the Ombudsman does not keep case records for the Department and maintains only those notes necessary to manage an ongoing case. The Office of the Ombudsman adheres to the Standards of Practice and the Code of Ethics of The International Ombudsman Association (IOA).

To protect the principle of privileged communications, the Department shall vigorously resist any effort to compel testimony or obtain notes or other records from an Ombudsman. To ensure maximum legal protection, the Ombudsman shall immediately contact the Legal Section upon knowledge or receipt of any document indicating efforts to compel testimony or obtain documentation.

Subject: Office of the Ombudsman	Number: SUP-12

Records, continued

The Office of the Ombudsman shall:

- Prepare a quarterly and annual statistical report for the Office of the Superintendent; and
- Protect the confidentiality and anonymity of the involved parties within submitted reports.

Supervisors

Supervisors shall:

- Ensure that employees under their supervision are aware of the Office of Ombudsman's confidential services in assisting with work-related problems;
- Provide support and commitment to the role and function of the Department's Ombudsman; and
- Be accessible to the Ombudsman to help in the resolution of work-related problems, as necessary.

Employees

Contacts with the Office of the Ombudsman need not be reported to a supervisor, as the program is accessible outside of the chain of command. An employee may contact the Office of the Ombudsman when seeking:

- Accurate information about Department policies, procedures, practices, or other issues;
- Informal advice on matters that they prefer to discuss without being "on the record"; and
- Assistance with work-related problems.

An employee who seeks the assistance of an Ombudsman may withdraw from the process at any time.

Contacts with an Ombudsman are voluntary and shall not jeopardize the employee's job security or promotional opportunities.

References: ADM-18Anti-Harassment/Sexual Harassment and Discrimination;
Bernard v. Commonwealth 424 Mass. 32 (1996);
The Administrative Dispute Resolution Act of 1995;
MGL c.112, §134, §135, §135A, §135B.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**TOP-01**

Subject:

Special Operations Command and Control

Purpose

To define the command and control of Special Operations and to provide guidance to Department members who are involved in any incident that involves (or may involve) the utilization of any Special Operations resource.

Policy

Special Operations may be comprised of the following Sections/Units/Teams:

- Special Tactical Operations Team;
- Crisis Negotiations Team;
- Mounted Unit;
- Canine Unit;
- Underwater Recovery Team;
- Special Emergency Response Team;
- Motorcycle Unit;
- Commercial Vehicle Enforcement Section;
- Collision Analysis and Reconstruction Section;
- Traffic Programs Section; and
- Motor Vehicle Regulatory Section.

The Colonel/Superintendent reserves the right to modify the Special Operations' Sections/Units/Teams.

For the purpose of command and control, members of Special Operations Sections/Units/Teams shall be accountable to one chain of command while performing Special Operations functions or assignments.

All Department personnel must be cognizant of the fact that tactical operations are inherently hazardous and require specific understanding of the risks, risk management, and the various capabilities and limitations of Department resources. Special Operations Section/Unit/Team Commanders and their members are specially trained and equipped to meet specific standards applicable to their assigned positions within the various disciplines.

Continued on next page

Activation Protocol and Response Procedures

Any emergency request for Special Operations resources shall include:

- The requesting agency's name;
- The requesting party's name and rank;
- The name and direct call-back number of the primary point of contact;
- The nature of the request; and
- The exact location of the incident and any designated staging areas.

Position	Responsibilities
Responding Member(s)	• Assess the situation, taking any actions necessary to eliminate immediate danger to others; • Contain and isolate the suspect(s) in the immediate area; • Advise the Desk Officer and request resources as necessary; • Gather and report as much tactical information as possible; and • If applicable, assume command and control until relieved by proper authority.
Station Desk Officer	• Advise Troop Duty Officer of request; and • Log entries into Daily Administrative Journal.
Patrol Supervisor	• Establish and secure perimeter as soon as possible; • Order evacuations, if necessary; • Establish liaison with local agency at scene; and • Ensure that only a single chain of command has control of the inner perimeter or scene.
Patrol Supervisor	**Additionally for significant events**: • Coordinate activities with outside jurisdictions (federal, state, municipal); • Establish a Command Post away from bystanders and the news media; • Assign a member as the media liaison until members from the Media Relations Section arrive; • Communicate accurate and current information on a regular basis to Troop Duty Officer; and • Upon conclusion of the incident, preserve the crime scene.

Continued on next page

Activation Protocol and Response Procedures, continued

Position	Responsibilities
Troop Duty Officer	• Notify GHQ Communications Section; • Dispatch Patrol Supervisor if necessary; • Log request in Daily Administrative Journal; • Notify Troop Commander. • Notify appropriate Special Operations Section/Unit/Team Commander or designee of the request; and • Activate/notify Special Operations Section/Unit/Team members and others as requested by Section/Unit/Team Commander or designee.
Special Operations Section/Unit/Team Commander or designee	• Contact initial requesting party to determine appropriate response; and • Brief the Special Operations Commander /designee to obtain operational approval.
Special Operations Commander/ designee	• Approve/deny activations/deployments; and • Contact Division of Field Services Commander.
Division of Field Services Commander	• Notify the Office of the Superintendent when appropriate; and • Activate other resources as needed.

Risk Management

Special Operations missions involve the likelihood of encountering potentially life-threatening hazards. All Special Operations Section/Unit/Team members shall exercise the best possible operational risk management strategies to:

1. Identify and assess hazards;
2. Develop controls to reduce hazards or risks; and
3. Use strategies to mitigate risk exposure and to safeguard the public and public safety personnel.

Removal from Assignment

Any member assigned to a non-biddable position with a Special Operations Section/Unit/Team may be removed at the discretion of the Colonel/Superintendent or designee.

Public Relations Requests

Requests for Special Operation resources for ceremonial, static or operational demonstrations, public relations displays, or other events shall be made in writing and approved by the Commander of the Division of Field Services.

Continued on next page

After Action Reporting

When so directed, Special Operations Section/Unit/Team Commanders are required to submit mission/incident specific After Action Reports to the Special Operations Commander/designee for review.

All After Action Reports shall be in a format approved by the Special Operations Commander.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

2149

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**TOP-02**
Subject:	
Special Tactical Operations (STOP) Team	

Policy

The Special Tactical Operations (STOP) Team shall:

- When requested and approved, assist members from the Department, local, state, and federal agencies; and
- Develop, under the direction of the STOP Team Commanding Officer, team specific Standard Operating Procedure (SOP) that shall be created, maintained, and updated as directed by the Special Operations Commander.

Purpose

To establish and define the role of the Special Tactical Operations Team within the Division of Field Services-Special Operations and establish guidelines for activation and utilization of their resources.

Definitions

Incident Command Post: A location where members may safely and effectively manage a scene, ideally equipped with a telephone, parking area, rest room, and effective radio communications for tactical team members.

Inner Perimeter: The immediate area of operations where violence or hostile actions are most likely to occur.

Outer Perimeter: A designated area outside the immediate area of operations which limits access and prevents harm to others.

Utilization of Resources

The STOP Team is available for:

- Emergency or critical incidents that may require a specialized response.

Operational Protocols

The designated Incident Commander (IC) shall:

- Attempt to isolate and contain the incident by establishing the initial inner and outer perimeter; and
- Continually assess the situation in conjunction with the STOP Team Commander or designee to determine the need for additional resources and to adjust tactics as required to resolve the incident.

Subject:	Number:
Special Tactical Operations Team	**TOP-02**

Operational Protocols, continued

Inner Perimeter:

- First responding members in the inner perimeter shall normally be replaced by STOP Team members once they arrive at the scene; and
- The Special Operations Commander or designee and STOP Team Commander or designee shall determine what personnel are required to safely manage the outer perimeter and scene.

Outer Perimeter:

- No Department member on the outer perimeter shall discharge their weapon once the STOP Team has assumed control and authority of the Inner Perimeter unless:
  - Ordered by the STOP Team Commander or designee; or
  - When necessary upon the threat of death or serious bodily harm.

Building Entry:

When the STOP Team has made entry into a building, all other responding Department members shall:

- Not aim, fire, or discharge a firearm into the building; and
- Take a position of cover.

The STOP Team Commander or designee shall:

- Have the primary responsibility to determine the type of equipment (including weapons) used by the STOP Team members.

Command and Control

When engaged in STOP Team operations, missions, and/or training the command and control concerning deployment and operational tactics utilized shall be:

- Determined by the STOP Team Commander or designee; or
- The Special Operations Commander or designee.

Evacuations/ Witnesses

In some instances, it may be necessary to evacuate nearby civilians. Witnesses or those who may provide situational awareness and/or intelligence may be requested to remain at or near the Command Post.

References: TOP-01 Command and Control.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**TOP-03**
Subject:	
Crisis Negotiation Team	

Policy

The Crisis Negotiation Team shall:

- When requested and approved, assist members from the Department and those from other local, state, and federal agencies; and
- Develop, under the direction of the Team Commanding Officer, team specific Standard Operating Procedure (SOP) that shall be created, maintained and updated as directed by the Special Operations Commander.

Purpose

To establish and define the role of the Crisis Negotiation Team within the Division of Field Services-Special Operations and establish guidelines for activation and utilization of their resources.

Definitions

Incident Command Post: A location where members may safely and effectively manage a scene, ideally equipped with a telephone, parking area, rest room, and effective radio communication for team members.

Negotiator: A specially trained member of the Crisis Negotiation Team who utilizes crisis management techniques in an effort to stabilize extremely dangerous and volatile circumstances.

Utilization of Resources

The Crisis Negotiations Team is available for:

- Crisis, hostage, or barricaded incidents that can potentially be resolved through dialogue; and
- Other special events/incident as assigned by Special Operations Commander or designee.

Operational Protocols

Crisis Negotiations Team shall:

- Utilize a philosophy of containment and negotiation;
- Assume control of the negotiations process once they arrive on-scene;
- Manage any personnel or individuals involved in the negotiations process; and
- Report to and remain operationally accountable to the Incident Commander.

Operational Protocols, continued

Useful information related to the operational area include:

- The layout of the building;
- Size and Number of rooms/spaces;
- Ventilation, food, and water supplies; and
- Observation points, approach, and escape routes.

Useful information related to perpetrator(s) and/or hostage(s) include:

- Names, number, age, gender, size, and physical condition;
- Behavior and emotional state (rational, tolerant, aggressive, ambivalent, etc.);
- Criminal record/weapons access/ownership;
- Purpose of act (terrorist, criminal, mentally disturbed); and
- Any stated plans, demands, or motivation.

Additional Response Guidelines

In addition to the response protocols outlined in TOP-01 Special Operations Command and Control, members shall follow these additional guidelines.

Position	Duties
Responding Member(s)	• Assess the situation, taking no aggressive action unless there is an immediate danger to others; • Contain and isolate the suspect(s) in the immediate area; • Attempt to slow the pace of events, and open and establish communication with suspect(s); and • Gather and report as much tactical information as possible.
Patrol Supervisor	• Request through the Troop Duty Officer the Crisis Negotiation Team; and • Designate a member to research utility shut-offs, if necessary;
Incident Commander	• Work with the Crisis Negotiation Team; • Attempt to maintain as much control as possible over the movements and behavior of the suspect(s); and • Attempt to defuse the situation while affecting the safe release of any hostages.

Subject:	Number:
Crisis Negotiation Team	**TOP-03**

Evacuations/ Witnesses

In some instances, it may be necessary to evacuate nearby civilians. Witnesses or those who may provide situational awareness and/or intelligence may be requested to remain at or near the Command Post.

References: ADM-07 Written Directives, Schedules and Forms;
TOP-01 Command and Control.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

2154

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**TOP-04**
Subject:	
Mounted Unit	

Policy

The Mounted Unit shall:

- When requested and approved, assist members from the Department and those from other local, state, and federal agencies; and
- Develop, under the direction of the Unit Commanding Officer, a unit specific Standard Operating Procedure (SOP) that shall be created, maintained and updated as directed by the Special Operations Commander in accordance with ADM-07 Written Directives, Schedules and Forms.

Purpose

To establish the role of the Mounted Unit within the Division of Field Services-Special Operations and establish guidelines for activation and utilization of their resources.

Utilization of Resources

The Mounted Unit is available for:

- Patrol and law enforcement services;
- Search and rescue;
- Crowd Control; and
- Other special events/incidents as assigned by the Special Operations Commander or designee.

Operational Protocols

The Mounted Unit Commander or designee shall:

- Determine the use of animals and equipment during inclement weather; and
- Consult with the Incident Commander regarding search patterns and/or other Special considerations.

References: ADM-07 Written Directives, Schedules and Forms;
TOP-01 Command and Control;
MPAC: 41.1.4.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

2155

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**TOP-05**
Subject:	
Canine Unit	

Policy

The Canine Unit shall:

- When requested and approved, assist members from the Department and those from other local, state, and federal agencies; and
- Develop, under the direction of the Unit Commanding Officer, a unit specific Standard Operating Procedure (SOP) that shall be created, maintained and updated as directed by the Special Operations Commander in accordance with ADM-07 Written Directives, Schedules and Forms.

Purpose

To establish and define the role of the Canine Unit within the Division of Field Services-Special Operations and establish guidelines for activation and utilization of their resources.

Utilization of Resources

The Canine Unit is available for:

- Conducting building searches for hidden offenders;
- Assisting in the arrest of dangerous or violent offenders;
- Tracking/locating suspect(s), lost and/or missing person(s);
- Locating criminal evidence or hidden instrumentalities;
- Locating cadavers;
- Detecting the presence of concealed narcotics, explosives, or arson related accelerants;
- Crowd control;
- Homeland Security related missions; and
- Other special events/incidents as assigned by the Special Operations Commander or designee.

Subject:	Number:
Canine Unit	**TOP-05**

General Protocols

- Only that amount of force that reasonably appears necessary to apprehend or secure a suspect shall be used. Handlers and their dogs are required to adhere to procedures that properly control their potential use of force and channel their specialized capabilities into legally reasonable crime prevention and control activities;
- Canine handlers are responsible for determining whether a situation justifies canine use and the appropriate special measures that should be taken;
- Employees shall not pet a canine except with the permission of the canine handler;
- No employee is to tease or agitate any canine unless performed as part of a training exercise;
- The canine shall not enter any State Police facility except for a specific police purpose;
- Whenever a canine is used in a special situation, Incident Commanders shall confer with canine handlers and members shall heed the directions of the canine handler;
- Canines shall not be handled by anyone other than their assigned handler, except in emergency situations;
- **No** commands shall be given to a canine by anyone other than the canine handler except in emergency situations; and
- **No** employee shall enter a canine cruiser while a canine is present, except at the direction and in the presence of the canine handler.

Building Search Protocols

Canines may be utilized for locating suspects in buildings or other structures. To optimize building searches, and if possible, the:

- Perimeter should be secured by the requesting patrol personnel;
- Owner should be contacted to ascertain the layout;
- Tenants, workers, or unnecessary personnel should be removed;
- Heating, air-conditioning, or other blowing units should be shut off so as not to interfere with the canine's scent;
- Entrances and exits should be monitored, and communications limited once entry is made by the search team; and
- Canine handler shall ensure notification has been made to all personnel prior to deploying a canine into any building or structure.

Tracking Protocols

Canines may be utilized for tracking. To facilitate tracking:

- Identify and mark the location where the subject was last seen;
- Avoid foot or vehicular movement in the immediate area;
- Set-up an initial perimeter to be searched; and
- Protect all items of clothing that shall be used for scent acquisition purposes.

Drug Detection Protocols

Public Facilities: Random exploratory sniffing of luggage, packages, or other inanimate objects may be conducted in public facilities such as:

- Airports/Transportation terminals (bus, train, marine);
- Commercial vehicle weigh stations; and/or
- Government buildings.

Public Schools: The use of drug detection canines in public schools is permitted only when authorized by the Division of Field Services Commander or designee, and if:

- The school administrator and the local police chief, if applicable, request and approve such use; and
- A search is limited to inanimate objects in public areas and the exterior of student lockers, unless reasonable suspicion exists to gain admission to an area.

Motor Vehicles: Drug sniffing canines may be used to sniff motor vehicles during:

- A commercial vehicle inspection; and/or
- A valid motor vehicle stop when reasonable suspicion exists to believe that the operator or passengers are in possession of illegal narcotics.

Use of Canines During Civil Disturbances

Use of Canines is governed by the Canine Unit SOP's in accordance with 550 CMR 6.08 (4-5), specifically:

- A member may not order the release of a dog to control or influence a person's behavior unless:
    - De-escalation tactics have been attempted and failed or are not feasible based on the totality of the circumstances; and
    - The measures used are necessary to prevent imminent harm and the foreseeable harm inflicted by the release of the canine is proportionate to the harm.
- If a law enforcement officer utilizes or orders the release of a dog against a crowd, the law enforcement officer's appointing agency shall file a report with the POST Commission detailing all of the measures that were taken in advance of the event to reduce the probability of disorder and all de-escalation tactics and other measures that were taken at the time of the event to de-escalate tensions and avoid the necessity of using said weapons, including a detailed justification of why use of said weapons was objectively reasonable.
- Canines should not be utilized for crowd control, restraint, or management of peaceful demonstrations, but may be deployed for crowd control, restraint, or management of peaceful demonstrations in isolated circumstances related to bomb detection, pursuit of suspects in buildings, and related situations. Utilization does not include circumstances in which the canine remains on a short lead in

close proximity to the handler and is well behind the line of contact between law enforcement and civilian personnel.

Canine Bites and Injuries

In the event that a Department canine bites or injures any party, the canine handler shall contact the Troop Duty Officer, who shall immediately dispatch a supervisor and Crime Scene Services to the scene to conduct an investigation in accordance with UOF-03 Use of Force Reporting and take color photographs.

The supervisor shall forward appropriate information including the SP 376 Use of Force Report to the Division of Field Services Commander and Canine Unit Commander prior to end of their shift.

References:
550 CMR 6.08 (4-5);
SP 376 Use of Force Report;
ADM-07 Written Directives, Schedules and Forms;
SOC-03C Response to Civil Disturbances;
TOP-01 Command and Control;
UOF-03 Use of Force Reporting;
MPAC: 41.1.4.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

2159

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**TOP-06**
Subject:	
Underwater Recovery Team	

Policy

The Underwater Recovery Team (URT) shall:

- When requested and approved, assist members from the Department and those from other local, state, and federal agencies; and
- Develop, under the direction of the URT Commander, a team specific Standard Operating Procedure (SOP) that shall be created, maintained and updated as directed by the Marine Unit or Planning, Preparedness, and Response Section Commanders in accordance with ADM-07 Written Directives, Schedules and Forms.

Purpose

To define the role of the URT within the Division of Homeland Security and Preparedness and establish guidelines for activation and utilization of their resources.

Utilization of Resources

The URT is available for:

- Underwater sweeps for hazardous or improvised explosive devices;
- Active search and rescue;
- Water-safety and survival instruction;
- Evidence location and recovery;
- Body location and extrication;
- Vehicle/vessel location and recovery;
- Underwater survey for security purposes;
- Underwater obstruction identification and removal;
- Homeland Security related missions; and
- Other special events/incidents as assigned by the Division of Homeland Security and Preparedness Commander or designee.

Operational Protocols

Because of the inherent risks involved in diving operations:

- Under most circumstances, no dive shall be undertaken until a diving supervisor and at least two (2) divers are present and prepared to dive;
- The URT Commander or designee at the scene shall make the final determination as to whether a mission shall be undertaken or terminated due to factors including safety, weather, currents, and sea state. The URT Commander or designee shall confer with the Marine Unit Boat Captain when conducting URT operations from vessels; and
- The URT Commander or designee shall be authorized to grant home based post mission gear decontamination and preventative maintenance.

Witnesses

In some instances, it may be necessary to evacuate nearby civilians. Witnesses or those who may provide situational awareness and/or intelligence may be requested to remain at or near the Command Post.

Command and Control

When engaged in URT operations, missions, and/or trainings, the command and control concerning deployment and operational tactics utilized shall be determined by the:

- URT Commander or designee

Activation Procedures

The URT is available for activation 24 hours a day.

For Emergency activations of the URT, contact the following:

- The Troop Duty Office of jurisdiction;
- GHQ Communications Section at 508-820-2121; or
- The Marine Unit (0700-2300) at 617-740-7820.

References: ADM-07 Written Directives, Schedules and Forms;
TOP-01 Command and Control.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**TOP-07**
Subject:	
Air Wing	

Policy

The Air Wing shall:

- When requested and approved, assist members from the Department and those from other local, state, and federal agencies; and
- Develop, under the direction of the Air Wing Commanding Officer, a unit specific Standard Operating Procedure (SOP) that shall be created, maintained and updated as directed by the Planning, Preparedness, and Response Section Commander in accordance with ADM-07 Written Directives, Schedules and Forms.

Purpose

To define the role of the Air Wing within the Division of Homeland Security and Preparedness and establish guidelines for activation and utilization of their resources.

Utilization of Resources

The Air Wing is available for:

- Search and rescue for lost, missing, or endangered persons;
- Photographic and video missions, documentation and video downlink;
- Motor vehicle enforcement and patrol;
- Incident command situations;
- Drug eradication efforts, including surveillance;
- Transportation of specialized equipment and personnel;
- Transportation of government officials;
- Criminal investigations;
- Dignitary protection;
- Fire services support;
- Homeland security related missions; and
- Other special events/incidents as assigned by the Division of Homeland Security and Preparedness Commander or designee.

Subject:	Number:
Air Wing	**TOP-07**

Operational Protocols

The Colonel/Superintendent, or designee, shall authorize all requests for out-of-state travel in department aircraft.

In accordance with Federal Aviation Regulations, the Air Wing Commander or flight crew members may decline, cancel, or terminate any request or mission due to factors including:

- Safety, weather, distance;
- Type of request beyond aircraft or members capability;
- Availability;
- Mechanical maintenance of the aircraft; or
- Determination that use of aircraft is not the appropriate resource after operational risk management assessment is completed.

This policy shall not preclude the use of the aircraft in any other circumstances at the direction of the Air Wing Commander consistent with the Air Wing SOP.

Command and Control

When engaged in Air Wing operations, missions, and/or training, the command and control concerning deployment and operational tactics utilized shall be determined by the:

- Air Wing Commander or designee; or
- Division of Homeland Security and Preparedness Commander or designee.

References: ADM-07 Written Directives, Schedules and Forms.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

2163

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**TOP-07A**
Subject:	
Small Unmanned Aircraft Systems (UAS)	

Policy

UAS missions shall:

- Not facilitate the use of any weapons and/or dispersal payloads;
- Comply with the United States Constitution, the Massachusetts Declaration of Rights, and all relevant and applicable laws and regulations; and
- Comply with all applicable Department Policies and Procedures, Rules and Regulations, and unit-specific Standard Operating Procedures (SOPs).

Purpose

The purpose of UAS Missions are:

- To define the operation of small Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) within the Department of State Police;
- To establish guidelines for the utilization and activation of UAS; and
- To develop, under the direction of the Department UAS Program Manager, unit-specific SOPs that shall be created, maintained and updated, as directed by the UAS Program Manager.

Definitions

Remote Pilot Certificate: A person acting as a Remote PIC of a UAS in the NAS under 14 CFR 107 must obtain a Remote Pilot Certificate with a UAS rating issued by the Federal Aviation Administration (FAA) prior to UAS operation.

Remote Pilot- in- Command (Remote PIC): A person who holds a remote pilot certificate with a UAS rating and has final authority and responsibility for the operation and safety of a UAS operation conducted under 14 CFR 107.

Small Unmanned Aircraft (UA): A UA weighing less than 55 pounds, including everything that is onboard or otherwise attached to the aircraft, and can be flown without the possibility of direct human intervention from within or on the aircraft.

UAS Program Manager: A Department member designated by the Colonel to oversee implementation, management, training, documentation and adherence to current FAA regulations for all Department-owned UAS. The UAS Program Manager shall create unit-specific SOPs and ensure the safe operation of all Department UAS.

Definitions, continued

Visual Observer (VO): A person acting as a flight crew member who assists the small UA remote PIC to see and avoid other air traffic or objects aloft or on the ground.

Utilization of Resources

Consistent with this policy, applicable laws and unit-specific SOPs, Department authorized UAS may be utilized for missions including, but not limited to, the following:

- Search and rescue for lost, missing, or endangered persons;
- Photographic and video documentation missions;
- Motor vehicle crash investigations / crash scene mapping;
- Criminal investigations and crime scene mapping;
- Tactical response missions (e.g., hostage rescue/barricaded subject);
- Providing an aerial visual perspective to assist officers in providing direction for crowd control, traffic incident management, special circumstances, and temporary perimeter security;
- Fire Services support;
- Homeland Security-related missions; and
- Other special events/incidents as assigned by the Division Commander, Unit Commander and/or UAS Program Manager or designee, consistent with and as permitted by law.

Prohibited Uses

Department UAS shall not be used for the following:

- To target a person based solely on individual characteristics, such as, but not limited to race, ethnicity, national origin, religion, disability, gender or sexual orientation;
- To harass, intimidate or discriminate against any individual or group; and/or
- To conduct personal business of any type.

Privacy

A UAS shall not be intentionally used for viewing, recording or transmitting images and/or video in a criminal investigation at any location or property where a person has a *reasonable expectation of privacy* unless:

- A warrant or court order has been approved for the search of the property;
- Consent by the owner or person responsible for the property is obtained; or
- Exigent circumstances exist, including but not limited to: search and rescue missions, tactical missions, crash scenes, crime scenes, fire scenes, hazmat scenes and natural disasters.

Subject: Small Unmanned Aircraft Systems (UAS)	Number: TOP-07A

Licensing, Certification and Registration

The Department UAS Program Manager shall:

- Ensure that all unit-specific remote pilots hold a Remote Pilot Certificate with a UAS rating issued by the FAA under 14 CFR 107; and
- Ensure that all UAS are registered with the FAA as required by 14 CFR 107.

Operational Protocols

The UAS Program Manager, the appropriate Unit Commander or the Remote PIC may decline, cancel, or terminate any UAS request or mission due to:

- Safety, weather, visibility;
- Type of request is beyond the UAS or member's capability;
- Availability;
- Mechanical maintenance of the UAS;
- Determination that use of UAS is not the appropriate resource after operational risk management or resource assessment is completed; or
- Determination that use of the UAS is in violation of this policy or Massachusetts General Laws.

All UAS missions will be flown in compliance with all current FAA Regulations including but not limited to 14 CFR 107. The Remote PIC has final authority and responsibility for the operation and safety of a UAS operation conducted under 14 CFR 107.

Training

The Department UAS Program Manager or designee shall:

- Ensure that all training and licensing is compliant with current FAA regulatory requirements including but not limited to 14 CFR 107.

Department members selected to be Remote PICs shall:

- Be properly trained and licensed as required by 14 CFR 107;
- Satisfy and maintain all the conditions of the Certificate of Authorization (COA) issued by the FAA if applicable;
- Have working knowledge of the airspace intended for operations and Air Traffic Control communication requirements; and
- Have the ability to obtain and interpret weather information.

Department members selected to be Visual Observers (VO) shall:

- Be properly trained according to standards set by the UAS Program Manager or designee that comply with FAA current regulatory requirements if any; and
- Satisfy and maintain all the conditions of the COA issued by the FAA if applicable.

Subject: Small Unmanned Aircraft Systems (UAS)	Number: TOP-07A

Mission Approvals

UAS mission requests shall be authorized by either:
- The appropriate Unit Commander or designee;
- The UAS Program Manager or designee; or
- The appropriate Division Commander.

Note: The Remote PIC has final authority and responsibility for the operation and safety of a UAS operation conducted under 14 CFR 107.

Authorized Equipment

Only Small UAS approved by the UAS Program Manager shall be authorized for use by members of the Department and/or for Department use.

Accident Notification and Investigation

In the event of a crash/incident involving fatalities, injuries, property damage, damage to the UAS or UAS fly-away, the Remote PIC shall:
- Report the crash/incident immediately to the appropriate Unit Commander and UAS Program Manager or designee;
- When applicable, notify the FAA in compliance with 14 CFR 107; and
- Complete and submit an incident report to the UAS Program Manager and appropriate Unit Commander.

The UAS Program Manager shall:
- Review all documentation and reports;
- Complete a summary report with conclusions and recommendations; and
- Forward all documentation through channels to the Colonel/Superintendent.

Digital Data preservation

All digital data including but not limited to photographs, video, and/or flight data shall be processed and maintained according to existing Department policies and preservation of evidence procedures.

Statistics, Records and Audits

The Department UAS Program Manager shall:
- Ensure that yearly statistics are kept for all UAS missions; and
- Ensure that flight and training records are properly maintained by the appropriate Unit Commander responsible for the use of the unit-specific UAS and forwarded to the UAS Program Manager.

References: 14 CFR 107;
TOP-01 Command and Control;
MPAC 41.1.5.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**TOP-08**
Subject:	
Marine Unit	

Policy

The Marine Unit shall:

- When requested and approved, assist members from the Department and those from other local, state, and federal agencies; and
- Develop, under the direction of the Marine Unit Commanding Officer, a unit specific Standard Operating Procedure (SOP) that shall be created, maintained and updated as directed by the Planning, Preparedness, and Response Section Commander.

Purpose

To define the role of the Marine Unit within the Division of Homeland Security and Preparedness and establish guidelines for activation and utilization of the Unit's resources.

Utilization of Resources

The Marine Unit is available for:

- Patrol and law enforcement services;
- Search and rescue;
- Waterborne surveillance/undercover operations;
- Underwater recovery (dive) operations support;
- Homeland security related missions; and
- Other special events/incidents as assigned by the Division of Homeland Security and Preparedness Commander or designee.

Operational Protocols

The Marine Unit Commander shall assign authorized Marine Unit members who are designated and trained to:

- Operate State Police vessels and their associated motors, trailers, and equipment.

For all Marine Unit missions a member shall be designated as Boat Captain per the Unit's SOP. The Boat Captain shall:

- Be responsible for the safety of the vessel and all individuals on-board.

The Marine Unit and the designated Boat Captain(s) shall:

- Collaborate with the Underwater Recovery Team Commander or designee to ensure a safe and efficient environment for all dive operations.

Subject:	Number:
Marine Unit	**TOP-08**

Command and Control

When engaged in Marine Unit operations, missions, and/or training, the command and control concerning deployment and operational tactics utilized shall be determined by:

- Marine Unit Commander or designee; or
- The Division of Homeland Security and Preparedness Commander ordesignee;

The Marine Unit retains administrative control and limited operational control over the Underwater Recovery Team (URT). The URT Commander retains tactical control during dive operations.

The Marine Unit has a stable of Reserve Officers comprised of sworn personnel that have been properly vetted and periodically assist the Marine Unit in carrying out tasking. The Marine Unit chain of command exerts operational and tactical control over these members only when they are assigned to the Marine Unit for specific missions.

Activation Procedures

The Marine Unit is available for activation 24 hours a day. The Marine Unit is staffed in Boston from 0700-2300 all year round. The Quabbin Reservoir Marine Patrol is staffed from 0700-Dusk from April-October. The Marine Unit is available in an on-call basis from 2300-0700. The Marine Unit monitors the Statewide Radio channel "State" and work with Station G for the tracking of resources and personnel. Emergent situations should be reported to the Marine Unit as soon as possible in order to prepare personnel and resources for rapid deployment.

For emergency activations of the Marine Unit contact the following:

- Station G over the State channel; or
- The Troop Duty Office of jurisdiction (to contact on call Trooper); or
- GHQ Communications Section: 508-820-2121; or
- The Marine Unit (07:00-23:00): 617-740-7820

References: ADM-07 Written Directives;
TOP-01 Special Operations Command and Control.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**TOP-09**
Subject:	
Incident Management Assistance Team	

Policy

The Incident Management Assistance Team (IMAT) shall:

- When requested and approved, assist members from the Department and those from other local, state, and federal agencies; and
- Develop, under the direction of the Unit Commander, a team specific Standard Operating Procedure (SOP) which shall be created, maintained and updated as directed by the Division of Homeland Security and Preparedness (DHS) Deputy Division Commander.

Purpose

To define the role of the IMAT within the DHS and establish guidelines for activation and utilization of its resources.

Utilization of Resources

The IMAT is available for:

- Large scale law enforcement operations;
- Lost or missing persons search and rescue missions;
- Extended recovery operations;
- Homeland Security-related missions; and
- Other special events/incidents as assigned by the DHS Deputy Division Commander.

Operational Protocols

IMAT members shall assist and advise on-scene Incident Commanders in the coordination and command and control of personnel and assets during the response to, mitigation of, and/or recovery from, an incident in a manner consistent with the Incident Command System (ICS) and the National Incident Management System (NIMS).

Responsibilities

Position	Responsibilities
IMAT Coordinator	• Shall be a commissioned officer from the DHS; • Shall be supported by members of the DHS IMAT; • Shall review the qualifications of all potential members and select Troop IMAT members who will also be available to the Department as IMAT members; • Maintain a list of all Department IMAT members, in combination with DHS IMAT members and Troop IMAT members; • Shall assist the Troop IMAT Officer in planning for IMAT support at planned Troop events; • Shall assist the Troop IMAT Officer with responses to unplanned Troop events; • At the request of the Troop IMAT Officer, shall provide the requesting Troop with IMAT support from the list of Department IMAT personnel for planned and unplanned events; • Shall plan IMAT training for all Department IMAT members; and • Shall identify and recommend IMAT equipment purchases through channels to the Colonel/Superintendent.
Division of Field Services Troop IMAT Officer	• Shall be a Commissioned Officer that is appointed by the Troop Commander from the Division of Field Services (DFS); • Shall identify and recommend to the Department's IMAT Coordinator a team of 5 subordinates as members of the Troop's IMAT; • Shall attend Troop planning meetings and report on anticipated IMAT staffing requirements to the Department's IMAT Coordinator; and • Shall make immediate notification to the Department IMAT Coordinator of Troop IMAT responses to unplanned events.

Responsibilities, continued

Position	Responsibilities
Department IMAT Members	• Shall provide the Department IMAT Coordinator with their current qualifications for selection and retention as Department IMAT members; • Shall respond to requests for Troop and Department IMAT responses; • Shall attend Department IMAT Training; and • Shall assist their Troop IMAT Officer when requested.

References: Homeland Security – National Incident Management System (NIMS) October 2017.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**TOP-10**
Subject:	
Special Emergency Response Team	

Policy

The Special Emergency Response Team (SERT) shall:

- When requested and approved, assist members from the Department or other local, state, and federal agencies; and
- Develop, under the direction of the Team Commanding Officer, team specific Standard Operating Procedure (SOP) that shall be created, maintained and updated as directed by the Special Operations Commander.

Purpose

To establish and define the role of the Special Emergency Response Team within the Division of Field Services-Special Operations and establish guidelines for activation and utilization of their resources.

Utilization of Resources

SERT is available for:

- Search and rescue efforts;
- Special event crowd management;
- Area security operations;
- Evidentiary searches;
- Fugitive searches;
- Prison and civil disturbances;
- Extended recovery operations support;
- Wilderness searches requiring advanced land navigation techniques;
- Homeland Security related missions; and
- Other special events/incidents as assigned by the Special Operations Commander or designee.

Civil Disturbance Response

SERT is a principal asset in response to planned mass demonstrations and civil disturbances. SERT actions will be in accordance with SOC-03C Response to Civil Disturbances, UOF-01 Use of Force and SERT SOP.

Operational Protocol

Search patterns and/or other tactical considerations shall be:
Determined by the Incident Commander; after
Consultation with the SERT Commander or designee.

Subject:	Number:
Special Emergency Response Team	**TOP-10**

References: ADM-07 Written Directives;
SOC-03C Response to Civil Disturbances;
TOP-01 Special Operations Command and Control;
UOF-01 Use of Force.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**TOP-11**

Subject:

Emergency Management Unit

Policy

The Emergency Management Unit shall:

- When requested and approved, assist members from the Department and those from other local, state, and federal agencies; and
- Develop, under the direction of the Commanding Officer, unit specific Standard Operating Procedure (SOP) that shall be created, maintained and updated as directed by the Special Operations Commander.

Purpose

To establish and define the role of the Emergency Management Unit within the Division of Homeland Security and Preparedness and establish guidelines for activation and utilization of the Unit's resources.

Utilization of Resources

The Emergency Management Unit is available for:

- Multi-agency resource management and coordination;
- Assistance and/or support with exercise planning and evaluation;
- Major event coordination support;
- Natural disaster response, recovery and mitigation coordination;
- Emergency evacuation coordination support;
- Advanced incident management training;
- Homeland security related missions; and
- Other special events and/or incidents as assigned by the DFS Special Operations Commander or designee.

Operational Protocols

The Emergency Management Unit shall:

- Serve in a liaison capacity between the Department and the Massachusetts Emergency Management Agency (MEMA) and other local, state, federal, and private emergency management partners;
- Ensure the liaison position is staffed when requested by the Director of MEMA during the activation of the State Emergency Operations Center; and
- Reports through channels to the Colonel/Superintendent.

References: ADM-07 Written Directives;
TOP-01 Command and Control.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**TOP-12**
Subject:	
Motorcycle Unit	

Purpose

To establish and define the role of the Motorcycle Unit within the Division of Field Services (DFS)-Special Operations and establish guidelines for activation and utilization of the Unit's resources.

Policy

The Motorcycle Unit shall:

- When requested and approved, assist members from the Department and personnel from other local, state, and federal agencies; and
- Develop, under the direction of the Unit Commanding Officer, unit specific Standard Operating Procedures (SOP) that shall be created, maintained and updated as directed by the Special Operations Commander.

Utilization of Resources

The Motorcycle Unit is available for:

- Escorts;
- Patrol and law enforcement services;
- Crowd management;
- Traffic control;
- Homeland security related missions; and
- Other special events/incidents as assigned by the Special Operations Commander or designee.

Operational Protocols

The Motorcycle Unit Commander or designee may decline, cancel, or terminate any request or mission due to:

- Issues involving safety, weather, or distance;
- Type of request beyond motorcycle or personnel capability;
- Availability; or
- Determination that the use of motorcycles is not the appropriate resource after operational risk management assessment is completed.

Subject:	Number:
Motorcycle Unit	**TOP-12**

Troop Assigned Motorcycles

Division of Field Services members assigned to motorcycle duty within a troop shall:

- Attend and successfully complete certification courses and periodic trainings as designated by the Motorcycle Unit Commander and approved by the Special Operations Commander.

References: Policy and Procedure TOP-01 Command and Control.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**TOP-13**

Subject:

Behavioral Observation and Suspicious Activity Recognition Unit (BOSAR)

Policy

The Behavioral Observation and Suspicious Activity Recognition Unit (BOSAR) shall:

- Have a strategic and interactive security platform, utilized in public settings, with the goal of identifying and disrupting individuals with hostile intent, as soon as possible in order to eliminate, or minimize, any harm to the public; and
- Be activated in any type of security function, location, or event. More importantly, its principals can be applied to daily law enforcement assignments.

Purpose

The main purpose of the BOSAR Unit is to serve as the primary plainclothes asset within the Department's large scale event security package. The main purpose of the BOSAR Unit is for officers to observe or detect "hostile" activity as soon as possible in order to eliminate, or minimize, any harm to the public.

Utilization of Resources

The BOSAR Unit is available for:

- Special event security;
- Fixed target security;
- SEAR Events and national media event security;
- Inaugurations;
- Dignitary visits;
- Large crowd attended events;
- Civil disturbances and/or protests;
- Area security operations;
- Homeland Security related missions; and
- Other special events/incidents as assigned by the Department, the Division of Homeland Security and Preparedness, and/or the Division of Investigative Services Commander, or the Department's designee.

Operational Protocols

Upon identifying a target for additional observation based on the target's activity and/or behavior, undercover officers should advise their BOSAR group supervisor and/or fellow team members as soon as practical and as soon as their concerns rise to the level that warrant additional assistance, surveillance, and/or action. Further, if an officer believes there ultimately is no concern or threat, that information should be communicated as well in

Subject: **Behavioral Observation and Suspicious Activity Recognition Unit (BOSAR)**	Number: **TOP-13**

Operational Protocols, continued

order to de-escalate the concern and re-focus assets. Unit members shall ensure that interactions, incidents, and observations are properly documented in ACISS.

References: Homeland Security – National Incident Management System (NIMS) October 2017.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**TRF-01**
Subject:	
Mission, Goals, and Objectives	

Policy

All members are responsible for facilitating the safe and expeditious flow of traffic.

Mission

To develop and implement data-driven, multidisciplinary strategies to maximize the safety of the users of the roadway system.

Traffic Law Enforcement

Goal

Minimize the incidence of offenses committed on the roadways and to promote voluntary compliance with traffic laws.

Objectives

- Minimize the number of crashes and the resulting fatalities, injuries, and property damage through uniform, consistent, and active enforcement;
- Maximize training, selective enforcement, and criminal enforcement to reduce the number of driver errors, traffic violations, and the overall crime rate; and
- Maximize the utilization of traffic data, crash reports, and citation information as key identifiers for personnel deployment and selective traffic enforcement.

Uniform Enforcement

Members shall enforce the motor vehicle laws of the Commonwealth in a uniform manner. Enforcement actions shall be guided by the Massachusetts General Laws, Code of Massachusetts Regulations, Federal Regulations, Department Policies and other lawful regulations related to the identified violation(s).

Uniform Enforcement, continued

The policy of uniform enforcement shall include, but not be limited to, the following traffic violations:

- Moving and non-moving violations;
- Reckless/aggressive operation violations;
- Hazardous and non-hazardous violations;
- Speed violations;
- Equipment/safety violations;
- Multiple violations;
- Violations resulting in traffic collisions;
- Operation of a vehicle by a driver under the influence of alcohol/drugs;
- Operation of a vehicle after driving privileges have been suspended or revoked;
- Public carrier/commercial vehicle violations;
- Off-road vehicle violations;
- Pedestrian and bicycle violations; and
- Newly enacted laws and/or regulations.

License Re-examination Referrals

Members shall notify the Registry of Motor Vehicles (RMV) when they identify operators who pose a risk to public safety as a result of their driving behavior or medical condition. Forms can be accessed via *PowerDMS/Department Forms/Traffic Programs Forms.*

Members should submit RMV form *Request for Immediate Threat License Suspension/Revocation* for any operator whose continued operation would constitute an immediate threat to the public safety.

Members should submit RMV form *Request for Medical Evaluation* for any operator that is physically or mentally incapable of safely operating a motor vehicle.

Traffic Crash Management

Goal

Minimize the incidences of loss of life, personal injury, and property damage resulting from crashes.

Objectives

- Maximize planning and coordinate programs by systematically obtaining pertinent data about collisions;
- Minimize the severity of personal injuries and safeguard the lives and well-being of persons involved in collisions by providing basic medical and other emergency services;
- Minimize the number of driver errors and traffic violations by determining the cause(s) of collisions and taking appropriate enforcement action; and
- Minimize secondary crashes and/or delays by clearing crash scenes as rapidly as possible.

Traffic Direction and Control

Goal

Minimize delays to motorists resulting from crashes, construction, or other impediments.

Objectives

- Maximize the presence of personnel and equipment at locations and times conducive to enhancing traffic safety and flow;
- Maximize the expeditious flow of traffic by maintaining a high degree of officer and cruiser visibility while on patrol or specific assignment;
- Minimize and prevent collisions by eliciting the assistance of transportation officials and other law enforcement agencies to resolve problems as quickly and efficiently as possible;
- Maximize the direction of traffic through the use of signs, signals, and mechanical devices to regulate, coordinate, and detour traffic; and
- Maximize inter-agency relationships by sharing knowledge and information with other law enforcement, transportation, and academic officials involved in the transportation system so as to be better able to identify opportunities and resolve problems as quickly and efficiently as possible.

Traffic Safety Education

Goal

Maximize the knowledge of motorists through Department announcements, direct motorist contact and provide information on risks, losses, and hardships associated with unsafe driving practices and/or equipment deficiencies.

Objectives

- Maximize the awareness among the general public of the risk of damage, economic losses, and hardships associated with crashes and/or arrests resulting from unsafe driving;
- Minimize crashes and traffic violations committed by the general public through comprehensive training and education programs in unison with media informational efforts; and
- Maximize the public's safety by providing education on the importance of safety precautions, and promoting good driving practices such as wearing safety belts.

Traffic Ancillary Services

Goal

Maximize service to motorists in need of aid or information in a timely manner.

Objectives

- Maximize public safety by diligently patrolling assigned areas and rendering assistance when needed;
- Minimize the dangers to a stranded motorist by obtaining appropriate and timely assistance;
- Maximize public acceptance and respect by courteously providing information; and

- Maximize public awareness of traffic safety information through Department Public Service Announcements (PSA's) and community relations efforts.

References Massachusetts Strategic Highway Safety Plan;
RMV Form- Request for Immediate Threat License Suspension/Revocation;
RMV Form- Request for Medical Evaluation;
MPAC: 61.1.5, 61.1.12.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**TRF-02**
Subject:	
Patrol	

Policy

The Department shall provide twenty-four (24) hour a day patrol coverage of state and interstate highways, as well as other areas of primary jurisdiction. The Department shall also be available to assist other agencies when required.

Patrol Function

The purpose of the patrol function is to:

- Protect life and property;
- Respond to emergencies and other calls for service;
- Investigate crimes;
- Ensure the safety of motorists and pedestrians; and
- Assist other members, police departments, and government agencies.

Deployment

Members may be deployed based upon the documented need for services. Criteria to be used for the assignment of personnel include, but are not limited to:

- Crime: Number of crimes, type, and severity;
- Calls For Service: Number of specific incidents, time, and type;
- Jurisdiction: Geography and demographics of the area;
- Crash Data: Number of crashes, type and severity;
- Roads: Type and miles of roadways; and
- Coverage: Sufficient patrols are available to ensure officer safety.

Roll Call

Supervisors or Station Desk Officers should conduct a roll call with shift members, preferably at the start of each shift. Roll call information may include items such as:

- Review of Department written orders and directives;
- Administrative messages;
- Legal updates;
- Patrol information; and
- Investigative and intelligence bulletins.

Patrol Responsibilities

The safety of members and the public are a paramount concern at all times.

Members shall;

- In accordance with TRF-07, Motor Vehicle Stops, prior to approaching any vehicle or engaging in patrol activities, members with access to an MDT, shall ensure related registration information is electronically documented and/or the location and registration information is broadcast to the desk officer and/or dispatcher via the radio system as soon as practicable. Members without access to an MDT shall broadcast the location and registration information to the desk officer and/or dispatcher via the radio system. Departures from this requirement may be authorized by supervisors when specific operational concerns exist AND must be documented via DAJ/Record of Investigation or To/From. The nature and duration of departure shall be documented;
- Maintain high visibility for general deterrence of criminal and traffic violations;
- In accordance with Department policy and MGL, identify and take appropriate enforcement action when applicable;
- Familiarize themselves with their patrol area including the location of hospitals, local police departments, and other such facilities;
- Utilize various routes of travel to promote the visibility concept and to minimize predictability;
- Remain in their assigned patrol area, unless otherwise authorized or directed;
- When practicable, check vehicles encountered parked within their patrol and/or traveled area, on the highway, and in rest areas (see ADM-46 Sexual Activity in Public Places), particularly at night and during periods of extreme or inclement weather to ascertain if the motorist/occupants are in need of assistance;
- Perform first responder duties by providing trained basic medical care until the arrival of more qualified emergency medical personnel;
- When appropriate, utilize issued fire suppression equipment until the arrival of fire services;
- Be alert to and report hazards within their patrol area, such as: road debris, inoperative traffic lights, missing traffic signs, fallen trees, or icy roads;
- If the condition or hazard is of an emergency nature, the member should remain at the scene until the situation has been resolved, or the member is relieved by another member, entity, or as ordered;
- Deliver emergency messages as approved by a Supervisory member to include, but not be limited to, next-of kin notifications in accordance with ADM-13 Notification of Medical Examiner and/or Next of Kin or other time sensitive law enforcement related message;
- Respond to alarms at Department and/or Commonwealth properties in accordance with established procedures;

Patrol Responsibilities, continued

- Maintain radio communication with barracks of jurisdiction advising the desk officer of self initiated activity that may require additional resources; and
- Monitor radio communications of local law enforcement, as practicable, and provide assistance in accordance with Department policy and MGL advising the desk officer of any self-initiated response.

Supervisors shall provide support to members to ensure their safety and efficiency while on patrol.

Desk Officer Responsibilities

Desk Officers shall be responsible for the following, but not limited to:

- Record member's Code 4 and Code 5 information when member's are signing on/off duty from assigned patrol areas. The Daily Administrative Journal (DAJ) entry should always accurately reflect what the member's Automated Vehicle Locator (AVL) will record;
- Enter the proper Roll Call information into the DAJ including member's patrol assignment and status;
- Monitor the proper radio channel(s) to maintain communication with Department members;
- Answering incoming phone calls to include:
  - Identifying location reached, rank and name (e.g. *State Police Holden-Trooper Smith*);
  - Classifying the nature of the incoming call as emergency/non-emergency; and
  - Communicating the Department's response to the call to the caller;
- Dispatch member(s) to incidents as necessary to provide safety and security to member(s) and the public. When available, a patrol supervisor should be requested to respond to incidents that may require a command element;
- Immediately dispatch members, including requesting local law enforcement, to emergency requests for assistance or activated emergency alarms from Department members;
- Notify or request assistance from the appropriate police department, fire department, emergency medical services or other resources as needed;
- Dispatch member(s) to address reported hazards/situations;
- Make appropriate notifications and request required assistance through the Massachusetts Department of Transportation Highway Operations Center;
- Record information in the DAJ on calls for service including, but not limited to the following:
  - Citizen reports of crimes;
  - Calls for service that are not crime related;
  - Incidents resulting in member(s) being dispatched or assigned; and/or
  - Incidents involving arrests, citations, or summonses as requested by initiating member.

Desk Officer Responsibilities, continued

- Each request for service or self-initiated activity entered into the DAJ should include, where applicable:
  - Date, time and location of request;
  - Type of incident reported;
  - Approximate time of dispatch and identification of member(s) assigned as primary and backup;
  - Name and address of complainant, if possible;
  - Approximate time of the member(s) arrival and return to service; and/or
  - Disposition or status of reported incident; and
- Communicate pertinent information to the Troop Duty Officer as appropriate.

Assisting Motorists

All members, regardless of duty assignment, shall be constantly alert for motorists who appear to need assistance. Whenever a disabled motor vehicle is observed, members should stop, unless a call or assignment prohibits them from doing so.

- Members are not required to perform mechanical work, change flat tires, jump-start vehicle batteries, unlock doors, etc.

If a disabled vehicle presents a clear and present danger, may create further traffic problems, and/or may increase the possibility of a traffic crash, it may be pushed off the primary roadway and onto the shoulder, median, or breakdown lane. When pushing a disabled vehicle, members shall:

- Ensure that sufficient care is taken to prevent unnecessary damage to both the disabled motor vehicle and Department motor vehicle; and
- Use only Department vehicles modified with extended front push bumpers, unless extenuating circumstances exist.

Depending upon time of day, weather, location of the vehicle or other variables, members should remain with the disabled vehicle and its occupants until assistance arrives, or they are assigned to a higher priority call for service.

- Members may allow stranded motorists and/or occupants to remain in a Department vehicle for safety and warmth; and/or
- Members may transport operators and/or occupants to another location for their safety or to a location where arrangements may be made for further assistance.

When encountering an unattended/abandoned motor vehicle members should:

- Stop and conduct a visual check of the vehicle; and
- Conduct an RMV and CJIS/NCIC inquiry into the status of the vehicle.

Assisting Motorists, continued

If the vehicle is properly registered and does not appear to be stolen or pose a risk to public safety, a courtesy check sticker should be completed and affixed to the vehicle, on the upper left corner of the rear glass or where it can be readily identified by other members. A log note shall be made in the DAJ by the reporting member, or the Desk Officer if the reporting member does not have immediate access to an MDT.

When asked to provide directions, guidance, or general information, members shall conduct themselves in a courteous and professional manner.

References

ADM-13 Notification of Medical Examiner and/or Next of Kin;
ADM-46 Sexual Activity in Public Places;
TRF-07 Motor Vehicle Stops;
Rules & Regulations Article 5.5;
Criminal Justice Information System (CJIS);
MPAC: 41.1.1, 41.1.2,41.2.4, 61.4.1, 61.4.2, 81.2.3, 81.2.4, 81.2.11, 81.2.13, 82.2.2.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**TRF-03**
Subject:	
Selective Traffic Enforcement	

Policy

The Department shall use special enforcement patrol duties as an effective technique to meet highway traffic safety goals and objectives.

The Troop Traffic Programs Officer shall document and report quarterly to the Traffic Programs Section Commanding Officer selective traffic enforcement activities conducted. This report shall be submitted no later than the last day of each quarter.

Annually, no later than December 31st, the Traffic Programs Section shall document an annual review of Department selective traffic enforcement activities.

Selective Traffic Enforcement

The primary purposes of selective traffic enforcement are to:

- Regulate traffic flow;
- Reduce traffic crashes; and
- Improve the safety of roads and highways.

Assignments shall be based upon:

- Crash data;
- Frequency of traffic violations;
- Traffic volume;
- Citizen complaints; and
- Any other pertinent information.

Traffic law enforcement depends upon the public and judicial acceptance of Department efforts. Selective enforcement shall be applied in a fair, impartial and unbiased manner to create a climate of compliance with motor vehicle laws.

The selective enforcement performance standards for members shall be based upon the goals and objectives of the mission.

It is important to understand that both a quantitative and a qualitative emphasis are integral parts of selective enforcement.

Troop Commanders

Troop Commanders may utilize any of the following selective enforcement techniques, or combinations thereof, based upon the Traffic Program Officer's and/or Traffic Program Section's reports:

- Aerial patrol by the Air Wing;
- Directed patrol utilizing Community Action Team(s);

- Speed reduction with speed measuring devices;
- Removing intoxicated drivers through saturation patrols, sobriety checkpoints, and other approved methods;

Troop Commanders, continued

- Commercial vehicle enforcement conducted by the Commercial Vehicle Enforcement Section (CVES);
- Joint operations in unison with other law enforcement agencies; and
- Providing education and information through electronic and print media releases and public presentations on traffic safety.

Traffic Programs Section

The Traffic Programs Section and other Department resources shall provide assistance and guidance to Troop Commanders on the selective enforcement activities to be conducted. This shall occur on a monthly basis and may include:

- Analysis of traffic crash investigations/reports data;
- Analysis of traffic enforcement activities data;
- Comparative analysis between traffic enforcement and crash data;
- Determining selective enforcement activities and programs success; and
- Review and revision of selective enforcement objectives.

Troop Traffic Programs Officer

The Troop Traffic Programs Officer is responsible for providing the traffic analysis for their respective Troop in conjunction with the Traffic Programs Section and other Department resources as stated above. The summaries shall include:

- Time and location of crashes;
- Causal factors; and
- Types of violations noted.

Station Commanders

Station Commanders shall utilize this traffic information for the scheduling of members for selective enforcement.

- Routine patrol assignments shall be planned based upon available Department resources in order to maximize the patrol effort of members not specifically assigned to other duties; and
- The assignment and deployment of members to selective enforcement should complement rather than replace regular patrols.

References: 20-DFS-012 Highway Safety Programs;
MPAC: 61.1.1, 61.1.10.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
December 6, 2021	**TRF-04**
Subject:	
Motor Vehicle Pursuits	

Policy

A motor vehicle pursuit is justified when the necessity of the apprehension of a suspect outweighs the risk created by the pursuit.

Members shall continuously evaluate all circumstances surrounding a pursuit. If the degree of danger to the public, the pursuit member(s), and/or the suspect(s) is greater than the necessity for immediate apprehension, a pursuit should not be initiated, or if in progress, should be terminated.

Definitions

Deadly Force: Use of force intended to inflict, or reasonably be expected to cause, death or serious physical injury.

Densely Populated Area: An established city or town that is thickly settled and/or comprised of a business district marked by compactness, pedestrian and vehicular traffic.

Objectively Reasonable: This term means that, in determining the necessity for and appropriate level of force, officers shall evaluate each situation in light of the known circumstances, including, but not limited to, the seriousness of the crime, the level of threat or resistance presented by the subject, and the danger to the officer, subject, or community. The reasonableness of a particular use of force must be judged from the perspective of a reasonable officer on scene, rather than with the 20/20 vision of hindsight. Determining reasonableness of force must allow for the fact that police officers are often required to make instantaneous judgments in circumstances that are tense, uncertain and rapidly evolving. The force used must be reasonable under the circumstances known to the officer at the time force is used. *Graham v. Connor* 490 U.S. 386 (1989)

Serious Bodily Injury: Injury that involves a substantial risk of death, permanent or protracted disfigurement, or extended loss or impairment of the function of a body part or organ.

Vehicular Pursuit: An active attempt by an officer in an authorized emergency vehicle to apprehend a fleeing suspect who is actively attempting to elude the police.

Prohibited Pursuits

Members **shall not** pursue a fleeing vehicle into another state, UNLESS:

- The reason for attempting to stop the motor vehicle is a felony **AND**
- The member is specifically authorized by the Troop Duty Officer to continue the pursuit into another state.

Pursuits of motorcycles, mopeds and motorized scooters **are prohibited** unless:

- the suspect poses an imminent threat of death or serious bodily harm to the public or officers; **AND**
- The member is specifically authorized by the Troop Duty Officer to continue the pursuit.

The Troop Duty Officer shall:

- Immediately assume command and control when circumstances result in a request for a CODE 1 regarding pursuit of a motorcycle, moped or motorized scooter; and
- Terminate the pursuit, unless the suspect poses an imminent threat of death or serious bodily harm to the public or officers.

Initiating a Pursuit

If a violator fails to stop when signaled to do so and operates in such a manner as to avoid capture, members must first recognize the potential risk to public safety before initiating a pursuit. Consideration should be given to tactics that reduce the opportunity for a suspect to evade apprehension.

If the degree of danger to the public, the pursuit member(s), and/or the suspect(s) is greater than the need for immediate apprehension, a pursuit should not be initiated or, if in progress, should be terminated.

Factors to consider include:

- Offense;
- Density of the populated area;
- Volume of vehicular and pedestrian traffic;
- Probability of apprehension;
- Type of vehicle being pursued;
- Availability of assistance;
- Speed and driving behavior;
- Presence of passengers;
- Location, visibility, weather, road conditions, and the time of day; and
- Other circumstances or conditions which mitigate or aggravate hazards associated with the pursuit.

Termination of Pursuits

Members shall immediately terminate a pursuit when any of the following conditions exist:

- When a pursuit for a civil infraction, misdemeanor or non-violent felony enters into a densely populated area or heavily congested roadway;
- If radio communications with the Troop Duty Officer cannot be established or lapse during the pursuit;
- When the initiating member or Troop Duty Officer evaluates or determines that the totality of the circumstances or risk of continuing the pursuit are outweighed by the risk to public safety; and/or
- When ordered to do so by the Troop Duty Officer or any Department member holding the rank of Captain and above.

Termination orders shall be immediately acknowledged.

When a member terminates a pursuit, he/she shall immediately deactivate all emergency visual and audible systems.

Pursuit Responsibilities

Position	Duties
Primary Pursuit Member	Shall: • Request a **CODE 1** and broadcast cruiser number, location, direction of travel, speed and traffic conditions; • Activate all emergency visual and audible systems; • Provide the original reason for the attempt to stop the motor vehicle, a vehicle description, and the visible-number of occupants in the vehicle; • Continuously broadcast the location, direction, speed, and road conditions; • Operate cruiser in accordance with General Order ADM-19A Vehicle Use and Maintenance, M.G.L. c. 89, s. 7B and continuously evaluate the risk to public safety; • Advise the Troop Duty Officer of any crashes; • Ensure that rendering assistance to injured parties takes precedence over the continuation of the pursuit; and • Conduct a comprehensive follow-up investigation in the event the operator eludes apprehension.
Barracks Desk Officer	Shall: • Verify the Troop Dispatcher has notified the Troop Duty Officer of the pursuit; • Receive, record, and coordinate information on the pursuit and the pursued vehicle with the Troop Duty Officer, Dispatcher and other law enforcement agencies; and • Ensure that all pertinent information regarding the pursuit is entered into the Daily Administrative Journal (DAJ) and forwarded to the Troop Duty Officer.

Pursuit Responsibilities, continued

Position	Duties
Assisting Pursuit Member(s)	Shall immediately: • Notify the Troop Duty Officer of their participation in the pursuit; • Maintain a safe distance behind the primary unit, but be close enough to provide aid; and • Assume radio communication if and when required. <u>Only three (3) State Police vehicles should engage in an active pursuit.</u> The Troop Duty Officer may permit additional State Police members to assist in a pursuit if he/she determines extenuating circumstances which warrant additional assistance. State Police vehicles not directly engaged in the pursuit, but in close proximity to the pursuit, shall immediately notify the Troop Duty Officer. These members shall position themselves on alternate/parallel roadways to provide assistance in the event the suspect eludes the pursuit member(s) or flees on foot; or as otherwise directed by the Troop Duty Officer.
Troop Duty Officer	Shall: • Immediately initiate a **CODE 1**; • <u>Personally broadcast</u> that they have assumed "command and control" of the pursuit; • Ascertain the cruiser number(s) of the involved member(s); location, direction of travel, speed, and traffic conditions; • Determine the original reason for the attempt to stop the motor vehicle; • Obtain the vehicle description, including plate number, if known, and number of occupants; • Continuously evaluate the risk to the public, and the pursuit member(s), as such risks relate to the necessity for immediate apprehension;

Pursuit Responsibilities, continued

Position	Duties
Troop Duty Officer	• Utilize State Police Air Wing (if available); • Direct State Police K-9 units to respond to the general area (if available); and • Direct State Police assets with tire deflation devices to respond to the general area, if available, and deploy device when applicable. **<u>Mandatory Termination</u>** In the event the pursuit member fails to transmit the required information to the Troop Duty Officer, said Troop Duty Officer shall terminate the pursuit. If the degree of danger to the public, the pursuit member(s), and/or the suspect(s) is greater than the necessity for immediate apprehension, a <u>pursuit should not be initiated, or if in progress, should be terminated</u>. **<u>Authority</u>** Regardless of the rank of the pursuit member, the Troop Duty Officer shall remain in command and control of the pursuit for the entire duration. **<u>Inter-Troop Pursuits</u>** The Troop Duty Officer of jurisdiction shall assume command and control once the pursuit enters their Troop. Adjoining Troop Duty Officers shall be notified of pursuits that are in close proximity to their jurisdiction and may enter into their area of responsibility. When a pursuit enters into a different Troop, the originating Troop Duty Officer shall remain in command and control until the adjoining Troop Duty Officer personally broadcasts that they have assumed "command and control" of the pursuit. **<u>Note:</u> Only the Troop Duty Officer from the originating Troop shall complete the pursuit evaluation.**

Pursuit Responsibilities, continued

Position	Duties
Troop Duty Officer	**Inter-Jurisdictional Pursuits** Troop Duty Officers shall notify other law enforcement agencies when a State Police pursuit is within their primary jurisdiction. The Troop Duty Officer shall factor into their pursuit continuation consideration any additional information provided by the other law enforcement agency. The Troop Duty Officer shall specifically state to the other law enforcement agency whether they are requesting their assistance or whether it is a courtesy notification with NO participation requested. Troop Duty Officers shall be responsible for the notification(s) but may authorize a designee to conduct the notification on their behalf. **Out of State Pursuits** If a felony has been committed, the Troop Duty Officer may authorize the pursuit member(s) to continue to pursue into another state. If this occurs, the Troop Duty Officer shall immediately: • Notify the law enforcement agency of jurisdiction and request their assistance; • Require that the first out-of-state law enforcement vehicle that joins the pursuit become the primary pursuit vehicle; • Direct the Massachusetts State Police vehicle to become a backup unit; and • Direct the MSP member(s) involved to return to the Commonwealth as soon as the pursuit investigation is terminated. **Crash/Injury Investigations** The Troop Duty Officer shall assign a supervisor to investigate all crashes and injuries associated with a State Police pursuit. A supervisor from the Troop in which the crash/injury occurred will be assigned the investigation.

Other Law Enforcement Agency Pursuits

Once a law enforcement agency notifies the State Police that they are in pursuit the caller must be identified and specifically asked:

- Whether they are making a request for State Police assistance; or
- Making a courtesy notification with NO State Police participation requested.

Once a request for assistance is made, the Troop Duty Officer shall determine if the State Police shall participate. If approval is granted, State Police member(s) shall act as a secondary unit to the other agency's officer unless otherwise directed by the Troop Duty Officer.

All State Police members directly or indirectly involved in a pursuit initiated by another law enforcement agency shall adhere to all of the requirements established in State Police General Orders, as well as Rules and Regulations.

Pursuit Driving Tactics

Reckless/Hazardous Driving – Members shall not duplicate the reckless operation displayed by fleeing suspects. Members are strictly prohibited from wrong way operation.

Deliberate Contact – A form of forcible stopping using a Department vehicle to intentionally make contact with a violator's vehicle in order to functionally damage or force the violator's vehicle to stop.

- Deliberate contact may be considered a use of deadly force;
- May only be initiated when the violator poses an imminent threat of death or serious bodily harm to the public or members;
- Should only be utilized when all other attempts to stop the violator's vehicle are, or would likely be, unsuccessful;
- Shall be utilized only when authorized and ordered by the Troop Duty Officer, Troop Commander or sworn Command Staff Member;
    - The exigent application of deliberate contact prior to authorization must be warranted by the immediacy of the exigency. (Ex: vehicle driving towards a crowd)
- All deliberate contact incidents shall be investigated as a use of force incident in accordance with UOF-03 Use of Force Reporting.

Tire Deflating Devices – Should be considered as an effective option for bringing a pursuit to conclusion for passenger vehicles only. The use of these devices is prohibited for motorcycles, mopeds, motorized scooters, buses, and trucks. (Refer to TRF-21 for additional details.)

Caravanning - Only three (3) State Police vehicles should engage in active pursuit. The Troop Duty Officer may permit additional State Police members to assist in a pursuit if he/she determines that extenuating circumstances warrant additional assistance.

Pursuit Driving Tactics, continued

Units Paralleling – Additional State Police members may operate with emergency visual and audible systems activated and assist by paralleling the pursuit or pre-position themselves at likely avenues of escape. These assisting units should refrain from direct/active pursuit unless specifically authorized by the Troop Duty Officer.

Passing – Attempts to pass another police vehicle are strictly prohibited, unless the police vehicle is disabled or ordered by the Troop Duty Officer.

Spacing – All units in pursuit shall space themselves at a safe distance to ensure proper braking and reaction time.

State Police Motorcycles – SHALL NOT be involved in a pursuit.

Unmarked State Police Vehicles – Members operating unmarked State Police vehicles shall only engage in pursuits if the vehicles are equipped with emergency visual and audible systems. Members shall allow a marked/semi-marked unit to assume the primary pursuit position at the earliest opportunity. The unmarked vehicle shall then become the assisting unit until an additional marked/semi marked State Police vehicle can assume the secondary role. Once three (3) marked/semi marked State Police vehicles have become actively involved in the pursuit, the unmarked vehicle should disengage from the pursuit unless specifically authorized by the Troop Duty Officer to continue involvement in the pursuit.

Non-Department Vehicles – Members are prohibited from initiating or engaging in an ongoing pursuit in a Non-Department Vehicle, unless an imminent threat of death or serious bodily harm to the public or officer(s) exists and/or so ordered by the Troop Duty Officer of jurisdiction.

Post Pursuit Documentation and Review

Position	Duties
Primary Pursuit Member	• Provide the Troop Duty Officer with relevant information so they can complete the electronic RAMS Pursuit Evaluation Form; and • Complete a written incident or arrest report.
Troop Duty Officer	• Ensure that the Desk Officer has entered all pertinent information into the DAJ and the entry is forwarded to Troop Headquarters; • Complete all required entries in the Troop Headquarters DAJ; • Ensure that the Troop Headquarters DAJ entry is included in the Daily AM Report; • Complete the electronic RAMS Pursuit Evaluation; and • Ensure a follow-up investigation occurs for suspects who elude apprehension.
Deputy Superintendent	• Appoint members to the Pursuit Review Committee.

Subject: Motor Vehicle Pursuits	Number: TRF-04

Post Pursuit Documentation and Review, continued

Pursuit Review Committee Members	• Examine each pursuit and ensure compliance with this policy and report their findings to the Deputy Superintendent; and • Refrain from reviewing any pursuits in which they were personally involved.

The Pursuit Review Committee shall conduct and document an annual analysis of all pursuits in accordance with Accreditation standards including, but not limited to identifying patterns or trends discovered and indicate whether training or policy revisions are needed.

References: ADM-19A Vehicle Use and Maintenance;
TRF-12 Traffic Crash Investigation;
TRF-21 Tire Deflating Devices;
UOF-03 Use of Force Reporting;
21-SM-04 TRF-04 Motor Vehicle Pursuits;
M.G.L. c. 89, §7B;
MPAC: 41.2.2, 41.2.3.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**TRF-04A**
Subject:	
Foot Pursuits	

Policy

Members shall continuously evaluate all circumstances surrounding a pursuit. If the degree of danger to the public, the pursuing member(s), and/or the suspect(s) is greater than the necessity for immediate apprehension, a pursuit should not be initiated, or, if in progress, should be terminated.

Criteria for Foot Pursuits

Mere flight by an individual not otherwise suspected of criminal activity shall not serve as the sole justification for engaging in a foot pursuit, or for committing significant Department resources.

Alternatives to Foot Pursuits

Foot pursuits are inherently dangerous and require heightened officer safety, situational awareness, and sound tactics.

Members should consider, if the situation allows, removing the keys from the ignition of Department vehicle and/or the suspect's vehicle before commencing the tracking of the suspect(s).

In deciding whether or not to initiate or continue a foot pursuit, a member should continuously consider reasonable alternatives to pursuit based upon the circumstances and resources available, including:

- Containment of the area;
- Saturation of the area with additional patrol personnel;
- K-9 support;
- Air Wing support;
- Apprehension at another time if the identity of the suspect is known or other information is available that would likely allow for later apprehension; and
- The need to immediately apprehend the suspect does not reasonably appear to outweigh the risk in continuing the pursuit.

The team concept of using two (2) or more officers should be used whenever possible.

If extenuating circumstances warrant continuation of a foot pursuit, it is generally recommended that a single member keep the suspect in sight from a safe distance and coordinate containment.

Termination of Foot Pursuit

Unless there is an immediate threat to another officer/member or the public, members should not initiate or continue a foot pursuit under the following conditions:

- The member has no portable radio, no means of communicating or loses communications with other members or barracks of jurisdiction;
- The member is alone and the suspect has fled into the woods or an unoccupied building;
- When two (2) or more officers/members become separated, lose means of communication with one another, or obstacles separate them to the degree that they cannot immediately assist each other should a confrontation take place;
- The member loses possession of their weapon or other essential equipment;
- When the member cannot articulate their location through means of landmarks or other identifiable means for responding members;
- When pursuing multiple suspects and the pursuing member(s) do not reasonably believe that they would be able to control the suspects should a confrontation occur; and/or
- When ordered to do so by the Troop Duty Officer.

Foot Pursuit Responsibilities

Position	Duties
Primary Pursuit Member	Upon the initiation of a foot pursuit, member(s) shall contact the barracks of jurisdiction, request a **CODE 1** and at a minimum, provide the following information: • Member's identification (cruiser number, call sign or name) and exact location; • If the member is in civilian attire, they should broadcast they are not in uniform and if possible a description of their outer garments; • Reason for the pursuit and current direction of travel; • Number and description of suspects; and • Whether the suspect is known or believed to be armed.

Foot Pursuit Responsibilities, continued

Position	Duties
Barracks Desk Officer	Shall: • Immediately notify the Troop Duty Officer of a foot pursuit; • Utilize technology including Automated Vehicle Locator (AVL) and mapping to coordinate containment perimeters with responding assets; • Direct additional barracks resources to the area to provide assistance; • Receive, record, and coordinate information on the pursuit and the pursued-suspect with the Troop Duty Officer and other law enforcement agencies; and • Ensure that all pertinent information regarding the pursuit is entered into the Daily Administrative Journal (DAJ)/ACISS.
Troop Duty Officer	Shall: • Immediately initiate a **CODE 1**; • Ascertain the member's identification (cruiser number, call sign or name) and last known location; • Determine the reason for the pursuit and current direction of travel; • Obtain the number and description of suspects; • Utilize State Police Air Wing (if available); • Direct State Police K-9 Units to respond to the area (if available); • Direct additional State Police tactical resources to respond to the area (if applicable); and • Ensure that all pertinent information regarding the pursuit is entered into the Daily Administrative Journal (DAJ)/ACISS. **<u>Mandatory Termination</u>** In the event the pursuing member fails to transmit or there is a loss of communication, the Troop Duty Officer shall terminate the pursuit upon next contact with the pursuing member who shall immediately acknowledge the termination order. Additional resources shall continue to respond to the area until the well-being of the pursuing member is verified and/or as directed by the Troop Duty Officer. If the degree of danger to the public, the pursuing member(s), and/or the suspect(s) is greater than the necessity for immediate apprehension, <u>a pursuit should not be initiated, or, if in progress, should be terminated.</u>

Subject:	Number:
Foot Pursuits	**TRF-04A**

References: *ADM-24 Department Radio Call Signs.*

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**TRF-05**
Subject:	
Traffic Incident Management	

Policy

The Department shall use Traffic Incident Management protocols to minimize the congestion and delay caused by highway incidents.

Traffic congestion causes safety concerns due to the increased risk of secondary crashes.

Every effort should be made to minimize this risk, in addition to the impact to public safety and the inconvenience to motorists of the Commonwealth.

Applicability

Every incident requires that certain Traffic Incident Management activities be performed. Even if the incident is minor, Traffic Incident Management protocols are applicable to some degree.

The system, whenever possible, should be applied to:

- Create familiarity with the system;
- Be prepared for escalation; and
- Increase awareness of the risks that exist in all incidents.

Goal and Objectives

Goal

Use "Quick Clearance" to restore the normal traffic flow as quickly and safely as possible.

Objectives

- Coordinate and expedite emergency response to incidents;
- Save lives, preserve property and minimize damage to the environment through the use and implementation of standard procedures and/or agreements;
- Improve incident scene management to facilitate quick clearance;
- Provide timely, accurate information to other agencies and roadway users about roadway conditions and alternate routes through the use of media, the Massachusetts Department of Transportation Highway Operations Center, and other systems; and
- Minimize the impact of non-recurring incidents through the use of pre-planned alternate routes.

Unified Command

Incidents occur without regard to jurisdictional boundaries requiring a well-integrated, unified command approach to managing the incident scene.

Roadway crashes, fires, and hazardous material incidents usually require a multi-jurisdiction, multi-agency response. Individual agency responsibilities and authority are normally confined by jurisdiction or function by statute.

Unified Command requires all responding agencies to have a functional responsibility that contributes to:

- Ensuring safety of ALL emergency responders;
- Determining overall incident objectives;
- Ensuring joint planning;
- Implementing strategy chosen for clearing the incident;
- Ensuring integrated tactical operations are conducted;
- Maximizing all assigned resources; and
- Re-opening the affected roadway as quickly and efficiently as possible to minimize traffic congestion delays resulting from the incident.

Traffic Incident Management Response Framework

Department members shall perform certain duties and responsibilities, such as first-on-scene or incident command, as necessary.
The following responsibilities are critical to initiating the appropriate response and successfully managing an incident:

Perform First-On-Scene Duties

- All members, when first arriving on the scene of a roadway crash, shall ensure the scene is safe and be prepared to assume the first-on-scene duties.

Evaluate the Incident

- Type of incident and potential number of injured, traffic conditions, lanes that are blocked, best access to the scene:
    - If a commercial vehicle (bus or truck) is involved, the Department of Transportation number is required.
    - In case of hazardous material releases: the type, estimated amount, tank rupture, and placard number is required.

Initiate Communication of the Incident

- Provide a brief description of the incident and if lane(s) of travel are required to be temporarily closed. Provide the exact location to include: route number, direction, town, exit number, mile marker, or landmark. Communicate the evaluation and the need for additional emergency and external resources to the barracks of jurisdiction.

Secure the Scene

- Secure the scene by whatever means available (cruiser, issued flares, etc.) to prevent further injury or property damage to the motoring public.

Perform First Responder Duties

- Provide trained basic medical care (e.g. CPR, first aid) until the arrival of more qualified emergency medical personnel.

Traffic Incident Management Response Framework, continued

Control Scene Access/Egress

- This may include providing escorts for emergency vehicles and equipment necessary for clearing the scene of the injured and any obstructions or hazards in accordance with TRF-22 Escorts and Relays.

Assume Incident Command (IC) Duties until Relieved

- The senior member at the scene shall assume Incident Command (IC) duties until the appropriate IC agency or higher ranking member arrives. In the event that an actual or serious threat of fire, explosion, or HazMat is encountered, the responsibility for the "immediate scene" shall fall to the Senior Local Fire Department Official. Department personnel should be aware that IC shall be transferred back to the Department once the fire, threat of fire or Hazardous Material has been removed and the scene deemed safe.

Support Unified Command as Necessary

- Paramount to the successful management of any critical incident is cooperation among all of the agencies participating in the operation. Department members shall be aware that IC might be rotated with an official of another agency (such as Fire or the Massachusetts Department of Transportation).

Implement Alternate Routes

- Redirect the flow of traffic from the incident when necessary. Members are reminded that when alternate routing is initiated, which may affect local communities, additional personnel may be needed to augment the local police department at strategic locations to safely move large volumes of traffic within the local community. The police department(s) of jurisdiction impacted shall be notified by the desk officer when alternative routing/traffic diversion may impact their area(s) of operation. When available, pre-planned traffic diversion plans should be utilized.

Assist the Public Information Coordinator

- The Department's Media Relations may dispatch qualified personnel to the scene of major incidents, if available, to support on-scene personnel. The IC should designate a Public Information Coordinator, normally a member from Media Relations when available, to interface with the media at the incident and identify a designated staging area for the media.

Conduct Incident Investigation

- The assigned patrol of jurisdiction, initial responding member or a member designated by the Incident Commander (IC) shall complete any and all reports required pursuant to established Department policy and procedure.

Traffic Incident Management Response Framework, continued

Participate in After-Action Review/Debriefing

- All applicable Department personnel involved should be made available for any after-action review to discuss their roles and actions during the management of the entire incident.

Traffic Control

When conducting manual traffic control, members should ensure that their presence and purpose are clear and obvious, and that they use traffic direction and control signals that are easily understood to ensure the safe and efficient flow of traffic.

Members conducting manual traffic direction/control at crash investigations or other roadway or critical incidents shall:

- Wear issued traffic vest or coat with high visibility side out and employ a flashlight when warranted;
- Adapt methods to changing and/or adverse road and weather conditions;
- Position themselves in a safe location so they are aware of and visible to oncoming traffic;
- Stand straight, with a military-like bearing facing traffic, and be alert to their duties and conditions around them;
- Use clear and simple hand/verbal signals to direct traffic;
- Start or stop one lane of traffic at a time on multiple lane roads, before proceeding to start or stop the next lane of traffic; and
- Request additional resources when necessary to ensure the safety of Department members and the public.

At the scene of critical incidents, members should assist by diverting vehicles around or away from the incident and allow medical and fire personnel room to operate. Roadway closures should be as short as possible and quick clearance techniques shall be employed whenever practicable.

Temporary traffic control devices, including portable signs, moveable barriers, and other apparatus, may be deployed to assist members in the safe and efficient flow and control of traffic. This is mainly applicable for pre-planned events, or long-term road closures.

Utilization of pre-planned traffic diversion plans may reduce the length of the road closure.

Subject:	Number:
Traffic Incident Management	**TRF-05**

References: Unified Response Manual for Roadway Traffic Incidents;
TRF 22 Escorts and Relays;
MPAC: 41.2.4, 61.3.2, 61.4.2, 81.2.5.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

2209

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**TRF-07**
Subject:	
Motor Vehicle Stops	

Policy

Necessary precautions shall be taken for every motor vehicle stop to ensure the safety of all. Members shall use these guidelines as well as their training and experience to determine specific actions for each situation.

Bias-Based Policing

All motor vehicle stops shall be in compliance with ADM-47 Bias-Based Policing.

Marked Cruiser Motor Vehicle Stops

Members in marked cruisers shall:

- Activate the emergency lights and siren, as necessary;
- Select a safe location, if possible, to stop a violator; and
- Position the cruiser behind the violator at a safe and reasonable distance, or as circumstances require.

Unmarked or Low-profile Cruiser Motor Vehicle Stops

Members operating unmarked/semi-marked cruisers should be aware that motorists might not recognize them as police officers and may refuse or be reluctant to stop. These motorists may drive to areas with increased population, illumination or to a local police station before feeling safe enough to stop.

Members should:

- If in uniform, wear the appropriate cover while signaling the motorist to stop during the contact;
- Request assistance from a marked cruiser if the motorist does not comply; and
- Advise the Troop of jurisdiction or GHQ Communications Center of the situation as people may use cellular phones to call 911 to ascertain the member's authenticity.

Felony Stops

Members making felony or high risk stops shall conduct the stop in accordance with established training guidelines, and if practical:

- Contact the barracks of jurisdiction Desk Officer giving the location, direction of travel, description of the vehicle, the number of occupants, and the reason for the stop;
- Request a Code 1;
- Position the cruiser in a manner that provides protection and cover; and
- Wait for backup to arrive prior to initiating the stop.

Assisting members should not give additional commands, unless necessary for officers' safety. They should remain in position to cover the primary member, who should issue the instructions to the vehicle occupant(s).

Approaching a Vehicle

When approaching a vehicle, members shall be aware of their environment and alert to oncoming traffic. Members shall:

- If in uniform, wear the appropriate cover, unless exigent circumstances are present;
- Ensure the portable radio is on;
- Approach in a manner that affords maximum protection; and
- Remain alert for any sudden or suspicious movement within the vehicle.

Operator Contact

Members shall:

- Speak to the operator from a safe position;
- In accordance with ADM-35 Body-Worn and Cruiser-Mounted Cameras, BWC/CMC members shall make every effort to inform civilians that they are being recorded at the earliest opportunity unless there is an immediate threat to the member's life or safety, making BWC/CMC notification impossible or dangerous. BWC/CMC members should make every effort to notify civilians with language such as "Ma'am/Sir, I am advising you that our interaction is being recorded."
- Request documentation related to the stop;
- Inform the operator of the reason for the stop;
- Remain professional and courteous;
- Avoid unnecessary conversation that may lead to verbal confrontations; and
- Assist the operator to safely re-enter the traffic flow.

Member Safety

Prior to approaching any vehicle or engaging in patrol activities, members with access to an MDT, shall ensure related registration information is electronically documented and/or the location and registration information is broadcast to the desk officer and/or dispatcher via the radio system. Members without access to an MDT shall broadcast the location and registration information to the desk officer and/or dispatcher via the radio system.

Subject: Motor Vehicle Stops	Number: TRF-07

Member Safety, continued

To maximize safety, the operator and occupants of the stopped vehicle shall be instructed to remain in the vehicle except for:

- An arrest;
- Situations where the member has specific articulable facts and reasonable suspicion that cause the member to be apprehensive for their safety or that of the public;
- Specialized enforcement functions;
- When conducting a field interview; or
- Other situations as necessary.

If a member is stopping a vehicle which they have articulable reason(s) to believe may pose a threat to the member or the public, they shall follow the felony stops procedure.

References:

ADM-35 Body-Worn and Cruiser-Mounted Cameras;
ADM-47 Bias-Based Policing;
TRF-04 Motor Vehicle Pursuits;
Comm. V. Gonsalves 46 Mass App. Ct. 186, 1999;
Comm. V. Williams 46 Mass. App. Ct. 181, 1999;
MPAC: 61.1.7, 61.1.8.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

2012

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**TRF-08**
Subject:	
Traffic Citations	

Policy

Traffic citations shall be issued in accordance with Policy and Procedure ADM-04 State Police Authority and Massachusetts General Law (MGL) c. 90C.

Issuance of Citation

The specific enforcement action taken should be predicated upon the offense. Traffic enforcement action should be taken at the time and place of the occurrence, unless:

- The vehicle could not be stopped;
- Additional time or information is necessary to determine the nature of the violation or identity of the operator; or
- Other extenuating circumstances exist at the time of the violation.

Members shall fill out all applicable fields within a citation including:

- The gender of the operator identified utilizing provided information;
- One applicable authorized code when identifying the operator's race; and
- If a non-inventory motor vehicle search is conducted the appropriate block shall be checked "yes or no."

Under no circumstances shall the race block contain unauthorized codes, remain unfilled, or contain inappropriate notations.

Issuing Member's Responsibilities

Members issuing citations shall:

- Utilize electronic citations as a primary means of issuing Massachusetts Uniform Citations. Paper citations may be utilized as an alternate means of issuing a Massachusetts Uniform Citation violation if the electronic citation is not available;
- Complete appropriate sections of the traffic citation accurately and legibly;
- Notify the violator of the specific violation(s) of law and whether the result of the violation is a civil citation, a warning, a criminal summons, or an arrest;

Issuing Member's Responsibilities, continued

- When applicable, explain the rights and requirements imposed by law to the violator upon arrest or issuance of the citation, prior to release. This shall include any optional or mandatory court appearance, whether a violator is allowed to enter a plea or pay a fine by mail, in person or on-line at the Registry of Motor Vehicles or court, and any other information that must be provided to the violator prior to release. An informational packet can augment but cannot substitute for the above information being provided verbally by members;
- For violations involving foreign diplomats/consular officials, military personnel, legislators and out of state residents, adhere to SOC-05 Special Considerations as appropriate;
- For violations involving juveniles, the issuance of citations shall be guided by M.G.L. and other Commonwealth regulations in effect at time of violation;
- Record citation information in the MSP MV Stop / Citation Data Entry located in CJIS Web as soon as practicable, but prior to placement of the physical citation in an unrestricted location;
- Forward the paper citations to the appropriate court/barracks of jurisdiction at or prior to the completion of their tour of duty. If unable to submit due to extenuating circumstance(s) the member shall submit upon the first next available time;
- Ensure the paper Department copy of the citation is submitted to the appropriate court officer; and
- Store completed paper citations in an identified secure area or within control of the barracks desk officer pending retrieval by the court officer on the next business day.

Members assigned to a barracks within the Division of Field Services shall utilize the station code of their assigned barracks in the approved format (e.g., A-1 Andover is SA-1). Members assigned to a section or unit not in Field Services shall use the station identifier approved by their Division Commander.

Court Officer's Responsibilities

Court Officers shall:

- Forward paper warning copies to the Registry of Motor Vehicles (RMV) forthwith;
- Mail or deliver paper civil infraction copies to the Registrar not later than the end of the sixth (6^{th}) business day after the date of the violations;
- Forward criminal complaint/summons to the court of jurisdiction no later than the end of the sixth (6^{th}) business day after the date of the violations; and
- File the paper Department copy.

Supervisor's Responsibilities

Supervisors shall:

- Review citations for accuracy, legibility, and compliance with statutory requirements; and
- Ensure that unacceptable/unprofessional patterns are immediately addressed.

Station/Section/ Unit Commander's Responsibilities

Station/Section/Unit Commanders shall:

- Maintain a control journal for all citation books received and issued;
- Review citations for accuracy, legibility, and compliance with statutory requirements;
- Review the citation data entered into the Citation Entry application by members under their command;
- Submit monthly/quarterly compliance reports as directed by the Traffic Stop Data Collection Technical Support Manual located on DocuShare;
- Ensure all paper citation copies are classified, distributed, and delivered to the RMV and the appropriate court(s), as required by statute;
- Retain all Department paper citation copies in barracks files for a period of three (3) years unless otherwise notified by the Legal Section; and
- Ensure that unacceptable/unprofessional patterns are immediately addressed.

Troop Traffic Programs Officer's Responsibilities

Troop Traffic Programs Officers shall:

- Maintain and forward up-to-date traffic/legal information as appropriate;
- Maintain a control journal for the issuance of citation books; and
- Maintain Monthly Troop Traffic Law Enforcement Statistical Summaries prepared in accordance with the requirements of the Division of Field Services.

Troop/Section Commander's Responsibilities

Troop/Section Commanders shall:

- Review monthly/quarterly compliance reports to ensure that the members under their command are in compliance with the provisions of this policy; and
- Ensure that unacceptable/unprofessional patterns are immediately addressed.

Division Commander's Responsibilities

Division Commanders shall:

- Establish internal guidelines for procedural review to ensure that the personnel under their command are in compliance with the provisions of this policy.

Recreational Vehicles

Members shall take appropriate enforcement action for violations committed by operators of off-road recreational vehicles (snowmobiles, dirt bikes, all-terrain vehicles, etc.,) observed and/or reported to them.

All MGL c. 90B violations shall be entered upon the standard RMV citation, or an application for complaint may be made with the District Court of jurisdiction.

The standard uniform citation can be utilized as a complaint application for a recreational vehicle operated on a public way in violation of MGL c. 90B §25.

Note: If needed, under the Executive Office of Energy and Environmental Affairs, the Massachusetts Environmental Police may be called for assistance at (800) 632-8075.

Voidance of Citations

Paper Citation Voiding

If an error is made while writing a paper citation, or if a citation becomes accidentally damaged, it may be administratively voided by the issuing member. The member shall:

- Print "VOID" on all copies of the citation;
- Provide a full explanation in writing (To/From) before the end of their tour of duty and submit it to their first line supervisor for review; and
- Record the voided citation in the MSP MV Stop / Citation Data Entry located in CJIS Web.

If satisfied with the explanation provided, the supervisor shall approve the "VOIDED" citation and the explanation for such action. The voided citation and explanation shall be returned to the Registrar forthwith.

eCitation voiding

If an error is made in the issuance of an eCitation, it may be administratively voided by the issuing member. The member shall:

- Provide a full explanation in writing (To/From) before the end of their tour of duty and submit it to their first line supervisor for review;
- The supervisor, if satisfied with the written explanation, shall electronically void the citation; and
- The To/From, shall be kept on file at the barracks and shall constitute the record of justification for the citation voidance. In order to ensure the Department retains the original To/From and to comply with records retention obligations, the To/From ***shall not*** be forwarded to the Registrar and/or the Merit Rating Board (MRB).

Subject:	Number:
Traffic Citations	**TRF-08**

References: ADM-04 State Police Authority;
SOC-05 Special Considerations;
MGL c. 90C Procedure for Motor Vehicle Offenses;
Traffic Stop Data Collection Technical Support Manual;
eCitation User Guide;
MSP MV Stop Date Entry User Guide;
MPAC 61.1.2, 61.1.3, 61.1.4, 82.2.4, 82.3.4.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**TRF-09**
Subject:	
Towing	

Policy

Public safety is the Department's primary concern and shall guide the application of this policy. When authorized to remove vehicles, members shall remove such vehicles to a location which shall ensure the safety and well-being of the occupants, security of the vehicle, and allow for safe and efficient flow of traffic.

All members and approved Tow Service Providers (TSPs) shall adhere to and comply with the Department of State Police SP-357 Tow Service Agreement (for those Troops/Tow Zones operating under the legacy Agreement), and/or the Massachusetts State Police Tow Contract (for those Troops/Tow Zones which have transitioned to the new Tow Contract).

Category I services are defined as Towing/Recovery/Service of vehicles or combinations ≤ 10,000 GVWR/GCWR, such as Passenger Automobiles, Light Trucks/Vans, Trailers, Motorcycles, Mopeds, or Motor Scooters.

Category II services are defined as Towing/Recovery/Service/HAZMAT of vehicles or combinations >10,000 GVWR/GCWR, such as Commercial Trucks, Truck Tractors, Tractor/Trailer Combinations, Trailers, Machinery, Campers/Motor Homes/Recreational Vehicles, and Buses.

Note: For those Troops under the legacy Tow Service Agreement providing for towing under Category II (Medium Duty) specifications, they shall abide by that Agreement.

Members assigned to Troop F shall adhere to Massport towing regulations.

Purpose

To establish and define guidelines for State Police members engaged in towing vehicles.

Causes for Removal

Members are authorized to remove (or cause to be removed) a vehicle found upon any way, or on private property without the consent of the property owner, when the vehicle is:

- Stolen or taken without the owner's consent;
- Disabled as to constitute an obstruction to traffic and/or is an obvious hazard;
- Improperly parked or standing in violation of a state or municipal law or regulation (i.e. within the limits of any State Highway for a period of time exceeding 24 consecutive hours);
- Not validly registered or insured in violation of law;
- In its current condition, is too hazardous or dangerous to be driven; and/or
- Impounded/towed pursuant to MGL or state or federal court order.

Additionally, members are authorized to remove (or cause to be removed) a vehicle found upon any way, or on private property without the consent of the property owner, when the operator is:

- Arrested;
- Not properly licensed;
- Impaired by the consumption of alcohol, drugs or any other substance, or by any medical condition;
- Unable or otherwise unfit to safely operate the vehicle,

AND

- There is no alternative operator present who could assume lawful custody of the vehicle; and
- After inquiry by the member, the owner or authorized driver cannot direct the member to dispose of the vehicle in some lawful and reasonable manner[1].

Additionally, members are authorized to remove (or cause to be removed) any vehicle found upon a road/state highway when adverse weather conditions or other emergency reasons necessitate the removal in the interest of public safety, or when requested by the Massachusetts Department of Transportation, or other agency having jurisdiction over maintenance of the roadway.

Any vehicles located on private property in situations not addressed above, including abandoned vehicles on private property, are a civil matter between the property owner and the vehicle owner, and shall be addressed as per MGL c.266 §120D.

Public safety is of paramount importance when considering the time, manner, and method of off-loading and/or towing a large vehicle. The key determinants are current and impending road, weather, and traffic conditions.

All crash/recovery scenes should be cleared as quickly as possible in order to return the highway to its normal traffic flow. If necessary, cargo may be pulled/pushed to adjacent shoulders/medians before the vehicle is towed.

[1] If the operator has refused a breathalyzer, the member must impound the vehicle for a minimum of 12 hours pursuant to M.G.L. c. 90, §24(1)(a)(4)(f)(iii).

Causes for Removal, continued

The off-loading and/or towing of large trucks involved in crashes and recoveries on high density/congested roadways should be avoided during peak commuter hours, as it may contribute to additional delays and/or secondary crashes.

Responsibilities of the Member Towing a Vehicle

Prior to notifying the tow company, members shall inquire whether the owner or authorized driver can direct the member to dispose of the vehicle in some lawful and reasonable manner, unless the operator has refused a breathalyzer test, in which case the vehicle shall be impounded for a minimum of 12 hours. Members shall also inquire if there is a preference for a particular tow company or roadside service organization. Factors to be considered with regard to the reasonableness of the manner proposed include, but are not limited to:

- Weather conditions;
- Whether traffic conditions require immediate removal;
- Time of day;
- Whether the situation requires expediency; and
- Whether the removal of the vehicle as proposed by the owner or authorized driver would be unreasonably long in the opinion of the on-scene officer(s)' and safety dictates its removal.

When no request for preference is expressed, the member shall inform the Station Desk Member who will dispatch a TSP from the Station's Tow Company List that is approved to provide the required service. For troops/tow zones operating under the new Tow Contract, the next-in-line TSP for that zone will be dispatched.

In the case of an incident which overlaps multiple tow zones within one barrack's area, or multiple barracks' areas, selection and dispatch of a TSP will be made by the barracks entering the call in RAMS.

Depending upon time of day, weather, or other variables, the member shall remain with a disabled vehicle and its occupants until assistance arrives, or until the member is assigned to a higher priority call for service. The member may transport the occupants to a safer location to make their own arrangements, if it is agreeable to the occupants.

If the member at the scene makes an informed observation that a particular on-scene TSP is unable to safely remove a vehicle he/she may request the services of the next in line approved TSP. If there is no next in line, the closest available approved TSP capable of handling the job shall be contacted.

When applicable, members shall inventory the towed vehicle in accordance with TRF-10 Vehicle Inventory.

Responsibilities of the Member Towing a Vehicle, continued

A towed motor vehicle shall only be placed on an investigative hold pursuant to:

- Melanie's Law (12 hour hold for Operating Under the Influence of Alcohol arrest with a breathalyzer refusal);
- Probable cause that the towed motor vehicle is a piece of evidence;
- Pending the application for and execution of a search warrant; or
- A directive from the District Attorney's Office, Attorney General's Office, or United States Attorney's Office.

A towed vehicle may not be held beyond ten (10) days, unless otherwise ordered in writing by a Court, the District Attorney's Office, the Attorney General's Office, or the United States Attorney's Office.

Any request for an investigative hold must be communicated to the TSP at the time of the tow. This notice will be documented on form SP-357C, with a copy maintained at the barracks of jurisdiction. The SP-357C shall be approved by a supervisor for all investigative holds, other than for Melanie's Law. In addition, the member must provide a copy of the approved written notice to the TSP prior to the end of his/her shift.

Responsibilities of the Station Desk Member

The Station Desk Member shall appropriately record the following via RAMS:

- The registration number and state;
- The location from which the vehicle was towed from including time and date;
- Make and description of the vehicle;
- The cause for removal;
- The name or identification number of the member or proper authority requesting such removal; and
- The towing company name, and the location to which the vehicle was moved.

Furthermore, the Station Desk Member shall properly classify tows/calls for service that are not provided by a contracted TSP, such as: owner request, motor clubs or help vans.

The member requesting the tow shall notify or cause to be notified, the owner of record as soon as possible, of the location of the vehicle and the reason for which it was towed.

Responsibilities of the Station Commander

The Station Commander shall ensure the effectiveness of the towing process by monitoring personnel and TSP resources operating under his/her command. The Station Commander shall:

- Establish separate lists for Category I and Category II operations;
- Establish a tow rotation within each tow zone having multiple TSP's;
- Rectify any substantiated claims of a missed or skipped call of a TSP;
- Request staging of tow trucks in specific areas for unusual demands for service;
- Assist TSP's with the administration of this policy and the associated towing contract(s);

Responsibilities of the Station Commander, continued

- Maintain records (SP-357C) of all vehicles held for investigative purposes;
- Ensure adequate log entries are made via RAMS; and
- Appoint a Station Tow Member to assist with the administration of this policy.

Responsibilities of the Station Commander ***in Troops/Tow Zones operating under the legacy Tow Service Agreement***

Station Commanders shall establish a Station Tow Company List based upon fair and equitable standards including, but not limited to: minimum response times, the maximum allowable number of tow companies, and the provisions of this policy.

Fair and equitable standards shall include, but not be limited to, the following:

- A consideration of the financial and administrative burden of maintaining and administering the Station Tow Company Lists;
- The public interest and necessity for the prompt removal of wrecked, crashed, and disabled vehicles from the roadway;
- The maximum number of tow companies on a Station Tow List shall not exceed ten companies unless authorized by the Troop Commander; and
- Any additional factors that a Station Commander deems reasonably necessary.

Station Commanders shall appoint a Station Tow Member to assist with the administration of this policy and to maintain records of all tow agreements and associated documents.

Station Commanders, in conjunction the Division of Administrative Services, will direct an investigation be conducted related to any SP-358 received alleging violations of the Tow Service Agreement SP-357.

Station Commanders shall be responsible for the oversight of station tow companies in their station areas and may suspend, terminate, and/or place on probation any station tow company consistent with the requirements of the State Police Tow Service Agreement SP-357.

Subject: Towing	Number: TRF-09

Responsibilities of the Troop Commander

The Troop Commander shall ensure the effectiveness of the towing process by monitoring personnel and TSP resources operating under his/her command. The Troop Commander shall:

- Order an immediate indefinite suspension without advance notice for an event where a TSP's actions have resulted in a threat to public safety or resulted in criminal action being sought against the company or any of its representatives;
- Notify the Division of Administrative Services of any suspensions ordered via the SP-358 process; and
- May establish amended Tow Zones for special events, natural or man-made disasters, states of emergency, weather events, or other unforeseen events in order to maximize public safety and reduce response times.

Complaints

All complaints, or allegations of violations of the Tow Service Agreement or Massachusetts State Police Tow Contract generated by members of the Department, the public, or a Tow Service Provider shall be immediately documented via an SP-358.

Complainants may obtain and submit a SP-358 by the following means:

- Accessing the State Police Tow Portal at https://www.mass.gov/state-police-towing
- Mail or hand-deliver to: Division of Administrative Services, 470 Worcester Rd., Framingham, MA 01702;
- Via email to towingresponsereports@pol.state.ma.us;
- By calling the Division of Administrative Services at (508) 988-7018; or
- Via fax to (508) 820-2359.

Subject: Towing	Number: TRF-09

Responsibilities of the Division of Administrative Services

The Division of Administrative Services (DAS) will provide administrative and fiscal oversight of all tow issues related to Troops/Tow Zones which have transitioned to the Massachusetts State Police Tow Service Contract. DAS shall:

- Establish and validate Tow Zones based upon input from Station Commanders relative to the number of crashes, requests for service, traffic volume, high-demand events or venues, and other measurable demands for service. Tow Zones shall remain fixed for the duration of the Tow Service Contract period. Tow Zones shall either be assigned to one specific approved TSP or to several TSPs based upon the contract award. If multiple companies are awarded a single zone, each shall be assigned on a per-incident rotation schedule;
- Recieve requests for inclusion in the Tow Contract;
- Evaluate new applications for Tow Contracts;
- Conduct independent, random audits of tow bills submitted by TSPs;
- Conduct initial and annual announced inspections of TSPs and prospective TSP's financial, insurance and employee records, as well as equipment and facility compliance;
- Conduct random unnanounced inspections of TSP's financial, insurance and employee records, as well as equipment and facility compliance; and
- Investigate all complaints forwarded via SP-358 regarding TSPs and this policy, determine violations of the Tow Contract, and take appropriate corrective action, if warranted.

Responsibilities of Tow Service Providers

TSPs must follow all applicable federal, state and local laws, and remain in compliance with the Tow Service Agreement (SP-357) and/or Massachusetts State Police Tow Contract at all times. Failure to maintain these standards may result in the immediate removal from all Department tow lists without advance notice.

References:

TRF-10 Vehicle Inventory;
SP-357 Tow Service Agreement;
SP-358 Tow Complaint;
Massachusetts State Police Tow Contract;
MGL c.90 §22B;
MGL c.90 §22C;
MGL c.159B §6B;
MGL c.266 §120D;
220 CMR 272;
720 CMR 9.04;
MPAC: 61.4.3;
Chapter 122 of the Acts of 2005.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**TRF-10**
Subject:	
Vehicle Inventory	

Policy

Any vehicle towed, or in the custody of the Department, shall be inventoried and properly documented in order to protect:

- The vehicle and its contents;
- The Department and tow company against false claims of lost, stolen, or vandalized property; and
- The member(s) and the public from dangerous items that might be in the vehicle.

When to Inventory a Vehicle

An inventory is a non-investigative procedure in which the contents of a vehicle are itemized, and the condition of the vehicle is noted.

The Department shall inventory any vehicle towed, removed, or impounded:

- As outlined within TRF-09 Towing;
- When involved in a crash, and the owner is unable to care for it;
- Pursuant to a lawful arrest when the vehicle would be left unattended; or
- As a seizure.
  - The vehicle is subject to statutory forfeiture or lawful seizure pursuant to a governmental interest, such as:
    1. A seizure pending forfeiture;
    2. Company or corporation distress warrant; or
    3. The vehicle was used in the commission of a crime, as an instrument of a crime, or is stolen.

The inventory process should be conducted at the scene before towing the vehicle. If the scene is not safe or practical, the process may be done at another location, however the inventory shall be done within a reasonable period of time.

Inventory Not Necessary

A motor vehicle inventory need not be taken if the vehicle is:

- Legally parked and locked;
- Abandoned and locked;
- Removed by a third party as outlined in TRF-09; or
- Disabled with the operator and/or occupants present

Subject:	Number:
Vehicle Inventory	**TRF-10**

Inventory Procedure

The standard inventory procedure shall consist of a detailed inspection of the interior and exterior of the vehicle for damaged and missing parts, as well as to locate and record the contents of the vehicle. The following areas shall be inventoried:

- The interior of the vehicle;
- The glove compartment and trunk (unless they are locked and there is no key available); and
- The exterior of the vehicle for missing or damaged parts.

The inventory listing of personal items and valuables shall extend to all storage areas and compartments that are accessible to the operator or occupants. This encompasses:

- All open areas, including the floor areas, the area in and around the instrument panel and the rear deck above the rear passenger seat, the open area under the seats, the glove compartment and trunk, and other places where property may be kept.

All closed but unlocked containers shall be opened, and each article inventoried individually.

Locked containers shall be inventoried as a single unit.

If an owner and/or operator requests to remove or entrust their possessions to another person, without it impeding the towing or impoundment process, such request may be granted, unless the member has probable cause to seize the items.

Search Warrants

A search warrant shall be obtained before the search of a locked container or forcing open a locked glove compartment or trunk, unless:

- Consent to open the container is obtained from its owner; or
- The member has probable cause to believe that such locked container shall put the member or others at immediate risk of injury or loss of life.

Responsibilities

Positions	Duties

Members	• Locate and secure any monies or articles of value that cannot be secured by the tow company;
	• Accurately record on the motor vehicle inventory form a complete listing of the general condition of the vehicle and its contents;
	• File the form in the barracks of jurisdiction;
	  o Records shall be kept for one (1) year; and
	  o Filed by date.

Subject:	Number:
Vehicle Inventory	**TRF-10**

Responsibilities, continued

Positions	Duties
Members	• A copy of the form may be filed with any report of investigation; • Make, or cause to be made, any necessary administrative journal entries; • Ensure that all articles taken for safekeeping are stored in an appropriate container and secured in the barracks of jurisdiction or with the owner; and • An article of value may be left with the vehicle, if the owner so requests, by storing it in the trunk.
Station Commanders	• Provide a central location for members to file the motor vehicle inventory forms, and periodically review the forms for compliance with this policy; and • Ensure that property secured during the inventory procedure is returned to the rightful owners, as appropriate, and not kept longer than necessary.
Troop Commanders	• Strictly enforce the motor vehicle inventory procedure in order to avoid arbitrary application of the policy.

References: TRF-09 Towing;
MPAC: 1.2.4;
Commonwealth v. Daley 423 Mass. 747 (1996);
Commonwealth v. Matchett 386 Mass. 492 (1982).

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
June 27, 2023	**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: License plate numbers of vehicles of interest, such as stolen vehicles or stolen plates, vehicles associated with missing or endangered persons, AMBER & Silver alerts, kidnappings, wanted fugitives, and others of specific interest to law enforcement that have a license plate number associated to them, including 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 managed, purchased, or subscribed to by the Department.

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 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 or locations 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 and operators 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 knowingly 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 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 conduct or authorize training for designated personnel in the use and operational protocols of the ALPR system;
- Coordinate with all Divisions and appropriate personnel to ensure that resources are available and deployed to meet Departmental needs;
- Maintain proficiency and familiarity with ALPR technology and systems, coordinate with other law enforcement agencies, and assist with investigations involving ALPR;
- Ensure that designated, trained personnel install equipment, check equipment 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 coordinate the purchase, deployment, and installation of ALPR systems and equipment;
- Conduct intermittent audits of ALPR system usage to ensure functionality and policy compliance; and
- Ensure that any substantive changes in policy or law are the subject of in-service training or bulletins.

Legal Considerations

In additional to the procedural safeguards outlined by this policy, members should conduct ALPR inquiries in the least intrusive manner as necessary and appropriate for the particular circumstances and should consider consulting with a prosecutor of jurisdiction regarding the potential need for legal process prior to accessing extensive or widespread ALPR data in active criminal investigations that do not involve exigent circumstances. See Commonwealth v. McCarthy, 484 Mass. 493 (2020).

Search Procedures

The Commonwealth Watch Center (CWC) and Commonwealth Fusion Center (CFC) shall serve as the primary ALPR resource for the Department. Search requests submitted to the CWC/CFC shall include, at a minimum:

- Case number or reference;
- Type of investigation or reason for request;
- Plate number(s) and vehicle description (if available);
- Requested search time period; and
- Requested search area (devices or region).

Searches of the ALPR system shall also observe the following guidelines:

- Properly complete justification fields;
- Limit search parameters to be reasonable and consistent with the geographic and temporal needs of the incident or investigation; and
- Document the parameters of the search.

The member who conducts or requests the search is responsible for ensuring that the procedures herein are followed. CWC/CFC may deny or refer to the ALPR Administrator any requests that they believe to be overly intrusive or otherwise inconsistent with law, policy, or best practices.

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, missing person, or kidnapping broadcasts or bulletins;
- Incapacitated or endangered persons;
- Be-On-Look-Out (BOLO) broadcasts or other public safety alerts;
- Investigation of terrorist or criminal offenses; or
- Wanted persons, arrest warrants, or search warrants.

Manual entries onto a Hot List shall be:

- Entered with the vehicle description, if available;
- Entered with a case number or reference;
- Updated or removed when information changes, is no longer current, or is no longer necessary or reasonable;
- Given special attention to rental and short-term use vehicles;
- Given special attention to incidents that may be quickly resolved;
- Entered with an automatic expiration date no longer than thirty (30) days; and
- Approved by a supervisor, except in exigent circumstances.

Manual Hot List Entries, continued

Designated and trained ALPR system users may conduct manual Hot List entries. All others should contact the Commonwealth Watch Center for assistance. The member who enters or requests a manual Hot List entry shall be responsible for ensuring that the information is removed per the guidelines above.

Mobile Operations

Department members operating a cruiser that is equipped with a mobile ALPR System shall:

- Ensure, at the start of each shift, that the ALPR system is activated and online, unless such use is incompatible with the member's duties at the time, the system is malfunctioning, or authorized by a supervisor;
- Ensure, 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

Prior to initiation of a stop or enforcement action based upon an ALPR hit or alert, members shall confirm the hit or alert, to include:

- *Verify the plate:* Visually verify that the vehicle plate matches the ALPR system's 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 that generated the hit/alert (e.g., is the vehicle still stolen), 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 information, records, or data from non-departmental ALPR systems.

Supervisors and analysts assigned to the Commonwealth Watch Center/Commonwealth Fusion Center and the ALPR Administrator may access non-departmental ALPR systems for official law enforcement purposes as authorized by this policy. 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, retention, and quality assurance standards than the Department's ALPR system. Members shall be mindful to preserve, export, or obtain copies of records or reports that are of known relevance to an incident or investigation prior to the expiry of the records.

Requests for Equipment and Accounts

Requests for the deployment or issuance of ALPR equipment or system accounts shall be directed through channels to the ALPR Administrator.

The ALPR administrator will approve, deny, or forward requests for deployment, equipment, and accounts as authorized under this policy, based upon the state-wide needs of the ALPR program, the availability of suitable equipment and personnel, and/or as directed by the Division Commander of Homeland Security and Preparedness.

Data: PII, Sharing, and Retention

License plate numbers and date/time location records collected by 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 or other investigative steps. 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) making a request for official purposes, 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 that are authorized to share data with the Department and/or access the Department's ALPR system shall be subject to the provisions of this policy or any superseding MOU or agreement in regard to use of the Department's ALPR system. Such outside agencies are responsible for their own designation, management, and supervision of that agency's system users, equipment, and any other systems or databases.

The ALPR system does not collect or retain video or audio recordings or intentional photographs of any individuals.

Retention of data shall be determined by the Department of Criminal Justice Information Services (DCJIS) policy. Members shall be mindful to preserve, export, or obtain copies of records or reports that are of known relevance to an investigation or prosecution prior to the expiry of the records.

2233

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 data 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 or legal proceeding.

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 sworn or civilian personnel whose positions and job duties justify such access, who have successfully completed a pre-employment background check, and who have completed appropriate training as designated by the ALPR Administrator, to include discussion of best practices and privacy considerations;
- Usernames and passwords to the ALPR system are not transferrable, must not be shared by Department personnel, and must be kept confidential; the only exception to this requirement is for mobile ALPR systems in pool cruisers in use by outside agencies, in which case the credentials can be used to activate the in-car camera system only and not to access or search the database; in such case the agency must maintain another tracking mechanism to identify the specific system operator, if needed;
- 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 monitoring, review, and audit at any time;
- Abuse of the Department's ALPR system will result in termination of system access and progressive disciplinary action; 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.

Reservations

These guidelines are set forth solely for the purpose of internal Department guidance. They are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter, civil or criminal, nor do they place any limitation on otherwise lawful investigative and legal prerogatives of the Massachusetts State Police or the Commonwealth of Massachusetts.

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
MPAC 41.3.9

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**TRF-12**
Subject:	
Crash Investigations	

Policy

To establish guidelines for traffic crash reporting and investigations.

Definitions

Commercial Motor Vehicle: A motor vehicle used in commerce, and designed or used to transport passengers or property, which has a gross vehicle weight rating (GVWR) of 10,000 or more pounds, or which is designed to transport more than eight (8) passengers (including the driver), or which transports hazardous materials and is required to be placarded in accordance with federal law.

Crash: A motor vehicle collision with any other vehicle, object, or person.

Crash Investigation: The systematic recording and examination of the involved vehicles, the roadway, and human factors, to determine the cause of the collision, contributing factors, and determination of violations of law.

Crash Reconstruction: The technical analysis of all available information and physical evidence to determine how and potentially why the crash occurred.

Crash Reporting: The basic data collection needed to identify the operators and the particulars of every crash referred to in Massachusetts General Laws (MGL) c.90 § 26.

Eligible Person: A resident of Massachusetts who is an operator or an occupant of a vehicle that strikes a deer.

Serious Bodily Injury: Injury that involves a substantial risk of death, permanent or protracted disfigurement, or extended loss or impairment of the function of a body part or organ.

Reporting Requirements

Members shall conduct an on-scene investigation and complete Registry CRA-65 Motor Vehicle Crash Police Report whenever a crash results in:

- A death;
- Personal injury;
- Any violation of law exists to include impairment due to alcohol or drugs;
- Any damage occurs to a Federal/State/Municipal vehicle; or
- Property damage per MGL c. 90 § 26 to include hit and run crashes.

Reporting Requirements, continued

For crashes not meeting the above requirements members should assist the operator(s) with the exchange of any pertinent information while continuously managing and expeditiously clearing the crash scene consistent with TRF-05 Traffic Incident Management. Members may utilize a SP 256 Crash Data Exchange Form to facilitate the exchange of pertinent information.

Station Desk Officer

Desk Officers shall:

- Dispatch members as needed to respond to the scene of any reported crash;
- Make an entry into the Daily Administrative Journal (DAJ) on all calls for service with appropriate findings;
- Make every attempt to identity callers for investigative purposes;
- Contact the Massachusetts Department of Transportation (Mass DOT) to respond with necessary equipment (such as arrow boards, cones, curiosity screens, message boards, signage, etc.);
- Notify the Troop Duty Officer of any crash where extended lane closures are anticipated and/or any crash involving serious or fatal injuries;
- Ensure Media Relations is made aware of any serious injury or fatal crash by faxing the SP 640 Serious Crash Fact Sheet directly to Media Relations and GHQ Communications; and
- Ensure the Registrar of Motor Vehicles is notified of all crash fatalities through the CJIS "FATAL" screen.

Responding Members

All responding member(s) shall:

- Exercise sound judgment in proceeding to the scene, but should respond expeditiously, to prevent any issues between the subjects involved or any secondary crashes from occurring;
- Position the cruiser and/or flares in such a manner as to provide maximum protection for the crash scene;
- Advise dispatch and/or the Troop Duty Office of any lane closures;
- Render first aid to injured subjects, pending arrival of emergency medical personnel;
- Direct traffic safely around the crash scene;
- Retain charge of the scene pending the arrival of the assigned patrol, department of jurisdiction, or any supervisory personnel;
- Ensure damaged vehicles are towed consistent with TRF-09 Towing;
- Prior to departing the crash scene, ensure roadway is clear of debris e.g., flares, cones; and
- Expedite quick road clearance consistent with TRF-05 Traffic Incident Management.

Primary Investigating Member's Responsibilities

In addition to the above duties the primary investigating member should:

- Conduct a preliminary investigation and comply with all reporting procedures;
- Take appropriate enforcement action when sufficient evidence exists;
- Notify the Desk Officer if the crash results in serious injury or death;
- When applicable, utilize findings and measurements determined by the Collision Analysis and Reconstruction Section (CARS) member as the official record for reference throughout the investigation;
- Request the Desk Officer make an entry into the DAJ documenting the time the crash was cleared and when traffic flow returns to normal; and
- Submit a CRA-65 Motor Vehicle Crash Police Report to a supervisor, within ten (10) days for approval.

Troop Duty Officer

Upon notification of a crash resulting in serious injury or death, notify:

- CARS;
- Crime Scene Services;
- The District Attorney's Office of jurisdiction; and
- Media Relations.

Troop Duty Officers shall follow the CARS call-out protocol set forth by the CARS Commander.

Note: Ensure that Mass DOT has been contacted to respond with necessary equipment whenever CARS members are responding to crashes on limited access highways.

Station Commander

Station Commanders shall:

- Review all reports for accuracy, completeness, and legibility; and
- Ensure the reports are forwarded to the Registrar of Motor Vehicles within fifteen (15) days.

Crash Reported at Construction Sites

When a crash occurs at the scene of a construction detail under the control and jurisdiction of the Department, the Desk Officer shall:

- Dispatch a patrol to investigate and take appropriate action; or
- Assign the member working the detail to investigate if that member is not involved in the crash, and when no patrol is available.

Reports for Death or Serious Injury

Motor vehicle crashes occurring on a public way resulting in death or serious injury require an incident report that may include:

- Observations from eye witnesses;
- Observations of hospital personnel;
- Forensic evidence of operation such as fingerprints, hair, blood, clothing fibers, etc. that place the occupant(s) accordingly;
- Seat positions;

Reports for Death or Serious Injury, continued

- Damage to the interior of the vehicle consistent with injuries to any occupant(s);
- Evidence from occupant protection devices such as seat belts and air bags;
- Evidence of contact with glass by any occupant in the vehicle;
- Any other pertinent information or evidence; and
- Preliminary findings from the CARS Reconstructionist.

Off-Road/ Recreation Vehicles

Off road recreational vehicle crashes occurring on public ways shall:

- Be investigated and reported on the standard CRA-65 Motor Vehicle Crash Police Report; and
- The standard uniform citation can be utilized as a complaint application for a recreational vehicle operated on a public way in violation of MGL c. 90B § 25.

Note: If needed, under the Executive Office of Energy and Environmental Affairs, the Massachusetts Environmental Police may be called for assistance at (800) 632-8075.

Crashes occurring on private property that involve a motor vehicle, or an off-road recreational vehicle, and resulting in death or serious injury shall:

- Be investigated and reported following the same reporting requirements and procedures set forth for death and serious injury crashes.

Crashes involving only property damage that occur on private property, not open to the general public, shall not require an investigation.

Collision Analysis and Reconstruction Section (CARS)

CARS may be used for the following purposes:

- When any crash involves a fatality;
- When any serious injury crash involves a strong possibility of criminal charges being filed;
- When any Department vehicle collision involves serious injury/death;
- When any serious injury occurs at a work zone where a member is working a paid detail;
- When any Department pursuit results in serious injury or death;
- Upon request by another police department/agency;
- Upon request of the District Attorney's Office, Fire Marshal's Office, or Attorney General's Office for assistance in forensic mapping of crime scenes; and
- As directed by the Troop/Section Commander.

CARS shall:

- Assist the primary investigator and shall not assume full responsibility for any investigation, unless ordered to do so by the Troop/Section Commander; and
- Forward an approved copy of the final report to the primary investigator for proper filing.

Local Cruiser Crash Investigations

Upon a request for a crash investigation involving a local police department, the request shall:

- Be made by the officer-in-charge (OIC) of the requesting department to the Troop Duty Officer.

Troop Duty Officers shall:

- Assign a supervisor (preferably of a higher rank than the officer involved) to conduct a crash investigation.

Investigating Members shall:

- Conduct an investigation and determine the cause;
- Take immediate enforcement action as necessary;
- Prepare an incident report; and
- Submit the incident report together with a CRA-65 Motor Vehicle Crash Police Report for review to the Troop Commander within seventy-two (72) hours of the crash.

Troop Commanders shall:

- Upon approval, forward a copy of the crash investigation to the local police department chief or designee for final disposition.

Crashes/ Commercial Motor Vehicles

Troop Duty Officers shall notify the Commercial Vehicle Enforcement Section (CVES) of all commercial motor vehicle crashes when they:

- Cause a major disruption of normal traffic;
- Involve serious injury or a fatality;
- Cause extensive property damage;
- Involve hazardous or radioactive materials;
- Involve violation(s) of law; or
- Are requested by the investigating member.

The "Truck and Bus Information" section of the CRA-65 Motor Vehicle Crash Police Report shall be completed by the primary investigator with CVES assistance.

Crashes with Deer and Disposition

Members should be aware that 321 CMR 2.04 allows an eligible person, to salvage the deer in accordance with certain stipulations. Members should:

- Ascertain if there is an eligible person who wishes to take possession of the deer;
- Advise the eligible person to immediately notify the Massachusetts Environmental Police;
- Ensure an entry is made into the DAJ that includes the name, address, and telephone number of the eligible person; and
- Notify Mass DOT if no eligible person is available or wishes to take possession of the deer carcass.

Release of Crash Reports

Private Individuals/Businesses

Private individuals, whether representing a business or themselves, are required to obtain crash reports from the Registry of Motor Vehicles.

Instructions for obtaining crash data can be found on the internet at: https://www.mass.gov/doc/rmv-request-for-copy-of-crash-report-form/download

State Employees/Representatives

Members shall release unredacted crash reports to:
Employees of MassDOT when an official(s) appears in person and is properly identified.

Representatives of private companies under State contracts responsible for repairs may be allowed to access information and records related to crashes available at Department facilities, under the following conditions:

- For the purpose of identifying monetary liability in crashes which resulted in damage to the infrastructure of the State highway system;
- Crash reports shall be accessed and copied only under the supervision of a Department member; and
- The Station Commander, or designee, shall be responsible for blacking out, the dates of birth and operator license numbers of all parties contained within the crash report.

Specific questions or concerns about the applicability of the Public Records Law or any other statute authorizing or restricting access to such material should be directed to the Department's Legal Section at (508) 820-2311.

References:

TRF-05 Traffic Incident Management;
TRF-09 Towing;
CRA-65 Motor Vehicle Crash Police Report;
SP 256 Crash Data Exchange Form;
SP 640 Serious Crash Fact Sheet;
49CFR part 172, sub-part F;
MGL c. 90B § 25;
MGL c. 90 § 26;
MGL c. 90 § 29;
321 CMR 2.04 Salvage, Disposition, and Possession of Deer Killed;
Criminal Justice Information System (CJIS);
MPAC: 61.2.1, 61.2.2, 82.2.1, 83.2.6.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**TRF-14**
Subject:	
Operating Under the Influence	

Policy

Members establishing probable cause of a subject operating a motor vehicle under the influence of alcohol and/or drugs should effect the arrest of said subject unless articulable extenuating circumstances prevent taking the subject into custody and necessitate an alternative means of enforcement at the time of the identified offense(s).

Definitions

Advanced Roadside Impaired Driving Enforcement (ARIDE): Training course intended to bridge the gap between SFST and DRE training providing officers with additional knowledge related to drug impairment.

Breath Test Operator (BTO): A member certified to administer a breath test in accordance with 501 CMR 2.00.

Drug: Any substance, when taken into the human body, which impairs the mental or physical abilities of the person taking it. This definition does not include the ingestion of ethyl alcohol.

Drug Recognition Expert (DRE): A person certified by the International Association of Chiefs of Police (IACP) as a Drug Recognition Expert whose primary function is to determine:

- Whether the subject actually is impaired; and if so,
- Whether the impairment is drug- or medically-related; and if drugs,
- The category or combination of categories of drugs that is the likely cause of the observed impairment

Officer-in-Charge of Instruments (OIC): A BTO, designated by a Station/Unit Commander responsible for maintaining the station/unit breath test devices. The OIC shall be trained in accordance with 501 CMR2.00.

Office of Alcohol Testing (OAT): Established within the Department of State Police Crime Laboratory that oversees the State's Breath Test Device Program and Breath Test Operator Training.

Preliminary Breath Test Device (PBT): A breath test device used to administer a screening test capable of quantifying the amount of alcohol in a breath sample or calibration standard.

Roadside Assessment: Test(s) designed to assist in the detection of impairment by a cause other than alcohol administered to a subject prior to arrest.

Definitions, continued

Standardized Field Sobriety Test(s) (SFST): Test(s) administered to a subject prior to arrest designed to assist in the detection of impairment due to alcohol.

Standardized Field Sobriety Test(s)

SFST(s) should be administered by the investigating member, if able, in accordance with training and the procedures outlined in the SFST Manual.

ARIDE trained members, when available, should provide additional roadside assessments to assist in determining possible drug categories contributing to impairment.

If available, a PBT Device, used as a Field Sobriety test, shall be administered as the last test.

Post Arrest Breath Tests

All post-arrest breath tests shall be conducted:

- By a certified BTO, however refusals may be entered by either a certified BTO or by a Department member not certified as a BTO;
- In accordance with 501 CMR 2.00 and Massachusetts General Laws (MGL) c. 90 § 24;
- In accordance with training and operational procedures developed by the OAT; and
- At one of the following locations:
  - The barracks of jurisdiction in which the arrest was made; or
  - At any barracks or other police department having an operational breath test device; or
  - The Department's Breath Alcohol Testing (BAT) vehicle.

Breath Test Results

Upon the successful completion of a breath test, the detainee will be notified of the results.

If the results are a 0.08% BAC or higher:

- Criminal charges shall be filed; and
- License seizure *only if* the detainee is in the possession of a Massachusetts driver's license.

If the results are between 0.079% and 0.060% BAC:

- Criminal charges shall be filed; but
- No seizure of license.

If the results are 0.059% BAC or less:

- There shall be a permissible inference that such detainee was not under the influence of intoxicating liquor, and they shall be released from custody forthwith per MGL c. 90 § 24, unless
  - Other charges, including but not limited to, OUI-Drugs support continued investigation and/or detention.

Subject:	Number:
Operating Under the Influence	**TRF-14**

Blood Tests

The preferred confirmatory test for OUI Alcohol is the breath test, but:

- Subjects arrested for OUI Alcohol and being treated at a medical facility licensed under MGL c. 111 § 51 may be offered an opportunity to submit to a blood test in lieu of a breath test; and/or
- Subjects arrested for OUI Alcohol and/or Drugs, may consent to a blood test to be taken at a medical facility licensed under MGL c. 111 § 51.

Specimen Collection

The collection of blood or urine samples related to an OUI case will:

- Be the responsibility of the arresting member or designee for oversight of the collection process; and
- Adhere to recovery of evidence guidelines contained within INV-10 Evidence Collection and Preservation.

OUI Drugs cases shall include the following forms with the case file:

- SP 603 Toxicology Request Form;
- SP 604 DRE Face Sheet (Preliminary) or Member's incident report (SP-12); and
- Evidence Submission Form (ESF).

DRE Evaluations

A DRE evaluation should be administered, when available and practicable, for subjects arrested for OUI Drugs or combination OUI Drugs/Alcohol.

DRE Request Criteria	An investigating member may request a DRE when: • The detainee is under arrest charged with Operating Under the Influence in violation of Massachusetts General Laws (MGL) c.90 § 24 and drug use is suspected; or • Blood Alcohol Concentration is not consistent with observed impairment; or • Any serious personal injury crash or fatal crash where impairment due to drugs is suspected.
Requesting a DRE	Members shall make a request for the assistance of a DRE to the Troop Duty Officer through the Troop Dispatcher.
Release from Custody	A detainee bailed from an operating under the influence charge may only be released to an unimpaired adult who agrees to take responsibility for the bailed detainee. The DAJ/ACISS shall reflect the identity of the person to whom the detainee was released. If a responsible adult is not available, the bailed detainee shall be placed into protective custody in accordance with DET-10, Protective Custody.
Protective Custody	The Arresting Member or Desk Officer placing a bailed detainee into protective custody shall: • Process the subject according to MGL c. 111B; • Re-enter the protective custody into the DAJ/ACISS; and • Ensure an SP 850 Protective Custody form is completed with a separate report and log entry made.

Responsibilities

Position	Duties
Arresting Member <u>OUI Alcohol</u>	• Advise the detainee of their rights and consequences as outlined in the Statutory Rights and Consent Form during the booking process; • If certified as a BTO, administer the breath test; • If not a certified BTO, ensure the breath test is administered by a certified BTO; • Complete all required documents and reports; • Ensure the detainee is provided suspension notification(s) if they fail the evidential breath test or refuses to submit to a breath test; • Pursuant to Melanie's Law, notify the tow company of a mandated 12-hour hold on a detainee's vehicle upon the breath test refusal of a detainee arrested for OUI Alcohol; and • If OUI Drugs is suspected, request a DRE evaluation.
<u>Combination OUI Alcohol/Drugs</u>	• Detainee's exhibiting signs of impairment for a combination of OUI Alcohol & Drugs shall be processed following procedures for OUI Alcohol; • If BAC is greater or equal to .08% continue with OUI Alcohol procedures unless the member believes a DRE evaluation would be beneficial; • If BAC is less than .08% and impairment is not consistent with BAC level, request a DRE and consider immediate threat; • If breath test is refused, request a DRE; • If impairment due to a combination of alcohol and drugs is suspected, both offenses shall be considered for charging; and • Complete all required documents and reports.
<u>OUI Drugs</u>	• Request a DRE; • Statutory Rights and Consent Form shall not be utilized; • Complete all required documents and reports; and • If warranted, follow Immediate Threat license suspension procedures.

Responsibilities, continued

Position	Duties
Breath Test Operator	• Administer a breath test in accordance with Chapter 90, §24 and 501CMR 2.00; • If the detainee refuses to submit to a breath test, ensure that the refusal is entered into the BATS; • If data entered into BATS is found to be incorrect, complete a BATS Data Correction Form, and fax to the RMV and OAT; • Complete all required documents and reports; and • Ensure detainee is provided suspension notification(s).
Drug Recognition Expert	• Ensure a call is assigned in the Daily Administrative Journal of the barracks of jurisdiction as a Call For Service: DRE Response/Eval; • Conduct an evaluation consistent with the twelve (12) step protocol as set out in the DRE Program; • Ensure that a parent, guardian, or legal custodian is present for juveniles who are under the age of eighteen (18) years; • Complete a Drug Influence Evaluation Narrative within the DRE system of record; • Submit a report for approval only to a MSP DRE Instructor holding the rank of NCO or higher; and • Submit approved DRE Face Sheet and Evaluation Narrative as a supplemental report to the court of jurisdiction;
Desk Officer	• Notify the bail commissioner and advise if the detainee requests to exercise their rights per MGL c. 263 § 5A; • Enter pertinent information related to the arrest and testing information into the DAJ/ACISS; and • Adhere to all requirements set forth in DET-06 Detainee Monitoring.
Supervisor	• Ensure compliance with this policy and the completion of all required documents and reports.
Troop Traffic Programs Officer	• Document date, time and location of each OUI related arrest and crash within their Troop.
Station/Unit Commander	• Designate OIC of Instruments and ensure they perform all assigned duties regarding Station/Unit breath test devices.

Responsibilities, continued

Position	Duties
Troop Commander	• Oversee OUI enforcement efforts within their Troop jurisdiction.
Officer-in-Charge: Instruments	• Provide guidance and assistance to BTOs and members entering refusal data; • Ensure detainee right to operate has been suspended if they fail the evidential breath test or refuses to submit to a breath test; • Ensure Station/Unit breath test devices, supplies, and current reference manuals are maintained and readily accessible; • Troubleshoot breath test devices and perform periodic tests as prescribed by OAT; • Maintain calibration stations for members who have been issued PBTs; • Coordinate with OAT and members for breath test devices certifications, calibration, repairs, and loaner/replacement units; • Maintain Station records of all periodic tests performed as prescribed by OAT; and • Testify as the Keeper of Records when required in-prosecutions within their jurisdiction.

References:

DET-06 Detainee Monitoring;
DET-10 Protective Custody;
INV-10 Evidence Collection and Preservation;
TRF-14B Preliminary Breath Test Device;
SP 850 Protective Custody Form;
Evidence Submission Form (ESF);
MGL c. 90 § 24, c.111 §. 51, c.111B §. 7, c.111B § 8, c.263 § 5A;
C.M.R 501 2.00 (Safe Roads Act);
Office of Alcohol Testing-Case Law Updates;
Statutory Rights and Consent Form;
BATS Data Correction Form;
Breath Test Operators Manual;
Preliminary Breath Testing Manual;
Standardized Field Sobriety Testing Manual;
RMV Form- Request for Immediate Threat License Suspension/Revocation;
Drug Recognition Expert Manual;
MPAC: 41.4.4, 61.1.11.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**TRF-14B**
Subject:	
Preliminary Portable Breath Test Devices	

Policy

Members shall utilize only devices approved and issued by the Traffic Programs Section which shall be operated and maintained in accordance with approved Department training.

Purpose

To provide guidance for the proper use, documentation, and maintenance of Preliminary Breath Test (PBT) instruments.

Definitions

Officer-in-Charge (OIC): The keeper of the breath test records for instruments assigned to their individual barracks or unit.

Office of Alcohol Testing (OAT): Established within the Massachusetts State Police Crime Lab (MSPCL) that oversees the State's Breath Test Device Program and Breath Test Operator training.

Preliminary Breath Test Device (PBT): A breath test device used to administer a screening test that is capable of quantifying the amount of alcohol in a breath sample or calibration standard.

Preliminary Breath Test Operator: A member trained to administer preliminary breath test.

Calibration and Certification

OIC and members issued a PBT Device shall:

- Successfully complete an operator training program;
- Adhere to Department of State Police guidelines for PBT Device maintenance and operation;
- Perform accuracy checks monthly according to Department of State Police guidelines;
- If not working properly, ensure that a PBT Device is taken out of service immediately;
- Notify Traffic Programs of a PBT Device taken out of service and in need of repair thus following repair arrangements made by OAT; and
- Ensure the PBT Device is certified annually, at the Office of Alcohol Testing, as directed by the Traffic Programs Section.

Subject:	Number:
Preliminary/Portable Breath Test Devices	**TRF-14B**

Records

OIC and members issued a PBT Device shall:

- Ensure records are maintained within their assigned barracks/unit per Department of State Police training; and
- Forward copies of the monthly accuracy checks to the Traffic Programs Section.

Traffic Programs Section

The Traffic Programs Section shall maintain an inventory of all issued PBT Devices and the inventory shall include:

- The member's barracks or unit assigned;
- Model and serial number of each PBT Device; and
- The Department Inventory Control number.

Testimony

Members should be aware that the following elements may be required in court testimony:

- Date, time, test number, subjects name and result of the blood alcohol contents percentage (BAC %);
- Department SP 691 Preliminary Breath Test (PBT) Log;
- The PBT Device was operating properly;
- The PBT Device was properly calibrated and certified;
- The training, qualifications and certification of the member; and
- PBT Device was the last field sobriety test administered.

Limitations

The acceptance of PBT Devices within the court system is dependent upon the member's:

- Proper care and effective use of the PBT Device;
- Appropriate PBT Device training and certification; and
- Use in combination with Standardized Field Sobriety Tests.

References:

SP 691 Preliminary Breath Test (PBT) Log;
Commonwealth v. Gary F. Goller, Trial Court Dept. Concord D.C. Docket No. 9647-CR-2063;
Commonwealth v. Blais 428 Mass. 294 (1998);
National Highway Traffic Safety Administration (NHTSA) *DWI Detection and Standardized Field Sobriety Testing.*

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

2050

Department of State Police
General Order

Effective Date:	Number:
May 25,2023	**TRF-15**

Subject:

Sobriety Checkpoints

Purpose

The primary purpose of Sobriety Checkpoints is to deter impaired driving, not to increase arrests. Police generally arrest impaired drivers detected at checkpoints and publicize those arrests, but arrests at checkpoints should not be used as a measure of checkpoint effectiveness.

Key Considerations

In the preparation and execution of any Sobriety Checkpoint, the following considerations shall receive special attention:

- When utilized, Sobriety Checkpoints shall be conducted in conformance with judicial guidelines;
- Motorist safety shall be prioritized;
- Motorist inconvenience shall be minimized;
- The action undertaken shall be in accordance with a written plan devised by supervisory personnel and developed prior to implementation of the checkpoint;
- Advance public notice shall be given to reduce motorist surprise, fear, and inconvenience; and
- A trained Commissioned Officer shall be in charge.

Site Safety

The Officer In Charge (OIC) of the Sobriety Checkpoint shall ensure compliance with the following Work Zone Safety Guidelines:

- Physical barriers shall not be used;
- Sufficient warning signs shall be placed ahead of the checkpoint to provide advance notice for on-coming vehicles;
- Signs should be illuminated or constructed of highly reflective material;
- Sufficient reflectors, or cones should be used to control traffic safely;
- Auxiliary and/or sufficient street lighting should be in place to illuminate the checkpoint;
- There shall be sufficient law enforcement presence to reduce fear and apprehension, minimize inconvenience, and ensure compliance;
- All officers shall be in an authorized uniform;
- All officers shall comply with work zone safety guidelines regarding the wear of an issued traffic vest or high visibility jacket;
- Officers shall position themselves so motorists can easily observe them;
- Visual stop/start commands should be given by either the officer or by signage;
- Marked cruisers shall be utilized as site safety vehicles;
- All safety vehicles shall have operable visual emergency warning devices; and

Site Safety, continued

- Safety vehicles shall be positioned in compliance with the pre-determined plan.

Vehicles shall be waved through the Sobriety Checkpoint without stopping when:

- Traffic is backed up to the safety officer;
- A commercial vehicle with a gross vehicle weight rating (GVWR) greater than 10,000 pounds causes sight obstructions;
- Vehicles transporting flammable liquids (including compressed gas as a motor fuel), hazardous materials or explosives as the cargo or a part thereof shall be allowed to pass through the checkpoint without stopping; and/or
- Due to articulable reasons, the member in a safety vehicle deems safety of the motorists would be best served by allowing traffic to pass.

Site Selection

Individual site selection shall be made based upon selective enforcement identifiers of alcohol related traffic crashes or prior OUI violations such as:

- Time;
- Day of the week; and
- Location.

Site selection data for each Sobriety Checkpoint shall be retained by the Troop Traffic Programs Officer for a minimum period of five (5) years.

Safety considerations for the site location should include:

- Motorist/officer safety;
- Sight visibility;
- Traffic volume and pattern;
- Operator reaction time; and
- Operator stopping distance.

Parking lots, rest areas, or wide shoulders immediately adjacent to the Sobriety Checkpoint should be available and accessible for use as a screening area. This will ensure that vehicles can be directed out of the normal flow of traffic without creating a traffic safety hazard.

Advance Notification

The OIC shall coordinate activities with Media Relations to ensure that:

- Announcements to the appropriate electronic and print media shall be made, at a minimum, three (3) business days prior to the implementation;
- The press release provides the overall purpose of the Sobriety Checkpoint, thereby allowing the Department to gain the public acceptance, support, cooperation, and voluntary compliance of the endeavor;
- The press release specifies the county the Sobriety Checkpoint shall be conducted in, but does not detail the precise location or hours of implementation; and
- Any inquiries pertaining to the Sobriety Checkpoint are referred to the appropriate Troop Commander.

Operational Plans

Individual Sobriety Checkpoint plans shall be prepared in advance of the date of actual implementation. These plans shall include, at a minimum:

- Date;
- Time and duration;
- Site selection and justification;
- Set patterns of vehicles to be stopped;
- Personnel, assignments, and responsibilities;
- Training for this particular sobriety check-point;
- Field sketch detailing the Sobriety Checkpoint logistics and site configuration;
- Notifications; and
- Equipment and materials needed.

These plans shall be strictly adhered to. There shall be no arbitrary or random modification of Sobriety Checkpoint procedures.

Officers may make suggestions for changes due to extenuating circumstances, but only the OIC can authorize and approve any changes in plans.

All officers shall be briefed and trained on details of the specific plan prior to the start of each Sobriety Checkpoint.

Operational plans shall be maintained at the Troop Headquarters and retained for a minimum period of five (5) years. A copy shall be forwarded to the Traffic Programs Section.

Site Configuration

Site configuration shall be as follows:

- Each Sobriety Checkpoint shall have a clearly marked warning sign;
- All signs, signals, markers, traffic cones, or reflectors shall be placed in accordance with the Work Zone Safety Guidelines;
- The position of the cones, or reflectors should guide vehicles to the appropriate lane of travel and are parallel to the stop location; and
- The position of the cones, or reflectors around the stop location should provide as much protection to the officers in that location as possible.

Stopping Vehicles

The selection of vehicles to be stopped shall be either:

- Every vehicle; or
- An objective set pattern, e.g., every other, every third vehicle, or other set number desired.

Vehicles stopped at the greeting officer should be met for a period of one (1) minute or less.

If there is reasonable suspicion, based upon articulable facts, that the operator and/or passenger(s) is committing or has committed an OUI violation or other violation of law, that vehicle should be directed from the normal flow of traffic and the offender(s) checked further.

Subject	Number
Sobriety Checkpoints	**TRF-15**

Cruisers

All Department vehicles shall be placed at Sobriety Checkpoint in such a manner as the OIC deems appropriate for safety purposes.

Personnel

The number of uniformed officers needed for a Sobriety Checkpoint may vary according to site and may take into consideration visible authority, motorist safety, and minimizing inconvenience.

There shall only be one (1) Commissioned Officer as the OIC of a Sobriety Checkpoint.

Responsibilities

Position	Duties
Division Commander of Field Services	• Annually, confer with the Traffic Programs Section regarding the efficiency of Sobriety Checkpoints; • Make a determination as to whether or not such checkpoints shall be utilized as a component of the OUI Countermeasures Program; and • Issue a Division Commander's Order directing all Troop Commanders to gather intelligence regarding potential sites for the deployment of checkpoints during the coming year, if such checkpoints are to be utilized.
Troop Commanders	• Shall designate a Commissioned Officer to conduct the site selection and operational planning for each Sobriety Checkpoint; • Approve the written operational plan and site selection; and • Designate a Commissioned Officer to be the OIC of the Sobriety Checkpoint.

Responsibilities, continued

Position	Duties
Sobriety Checkpoint OIC	Shall ensure: • The safety of all motorists and officers at the checkpoint; • Motorists are directed to the screening area by at least one (1) officer; • At least one (1), preferably two (2) officers interact with motorists during the screening process; • Motorists not arrested are released as quickly as possible; and • Arrested motorist's vehicles are inventoried and towed, if applicable, in accordance with TRF-14; and • If practical, the vehicle may be released to a licensed and sober operator, before towed from the screening area, if the detainee submits to a breath test.
Safety Vehicle Officer(s)	Shall: • Assist with the setup of the work zone prior to the start of the checkpoint; • Observe traffic for vehicle operation indicating OUI; • Observe traffic to forewarn other officers and motorists of approaching dangerous drivers; • Observe traffic for violations of law and notify the OIC; • Ensure that visual warning devices are activated; and • Monitor traffic for backup. Note: Speed measuring devices may be used by the safety officer.

Subject	Number
Sobriety Checkpoints	**TRF-15**

Responsibilities, continued

Position	Duties
Sobriety Checkpoint Greeting Officers	Shall: • Be courteous and polite when interacting with motorists. The element of voluntariness reduces the intrusiveness of the procedure; • All contacts should be kept brief, with a short greeting such as "Good evening, this is a State Police Sobriety Checkpoint. Sorry for the inconvenience, thank you." The inconvenience to motorists must be minimized; • If reasonable suspicion that an OUI offense or any violation of law has occurred, direct the vehicle to the screening area; and/or • Ensure the safety of motorists being checked further by directing them to an appropriate location to park in the OUI screening area.
Sobriety Checkpoint Screening Officers	Shall: • Minimize the inconvenience of motorists by screening them for OUI as efficiently as possible and administering the Standard Field Sobriety Tests, roadside assessments and/or preliminary breath test device (PBT); and • If probable cause is established for OUI, the member shall arrest the subject, barring extenuating circumstances dictating alternative enforcement action(s).

References

M.G.L. c. 90 § 24;
Commonwealth v. McGeoghegan 449 N.E.2d 349;
TRF-09 Towing;
TRF-10 Motor vehicle Inventory;
TRF-14 Operating Under the Influence;
MassHighway Work Zone Safety Guidelines;
NHSTA Countermeasures That Work, Fifth Edition, 2010;
MPAC: 61.1.6, 61.1.10, 61.1.11.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

2256

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**TRF-16**

Subject:

Speed Measuring Devices

Purpose

The Department shall use speed measuring devices as part of the strategy to reduce motor vehicle crashes and enhance public safety within the Commonwealth.

Members shall only use Department issued speed measuring devices for which they are trained and maintain a current certification.

Definitions

Calibrated: When the device is taken to a contractor that issues a calibration certificate which verifies proper functionality.

LIDAR Device: A speed measurement device that uses light detection and ranging to measure multiple distances and calculate speed.

RADAR Device: A speed measurement device that uses radio detection and ranging to measure relative changes in motion and calculate speed.

Tested: A procedure that checks on the functionality of the device as recommended by the manufacturer and training.

Tracking History: An essential process that confirms observations that a specific vehicle and operator did in fact commit the violation.

Use

The safety of the member, violator, and motoring public shall be of concern whenever selecting locations and conditions for speed enforcement operations.

Testing, Calibration & Certification

All members using a LIDAR Device, RADAR Device, or any other speed measuring device should successfully complete the National Highway Safety Administration's Core operator training program and receive specific certification in the respective speed measurement category prior to use.

- Members should reference manufacturer's guidelines for the maintenance and operational procedures of the device(s);
- Members shall test their speed measurement device prior to usage to ensure accuracy.
    - If the device fails an external or internal test it shall be taken out of service immediately until repaired; and
- LIDAR and RADAR devices shall be calibrated annually, as directed by the Traffic Programs Section.

Records

Calibration certificates shall be maintained by the Station/Unit Commander or designee and the Traffic Programs Section. The Traffic Programs Section will be notified of all maintenance and calibration of speed measurement devices used by members of the Department.

Speedometer

Speedometers should be checked by using a speed measuring device:

- Periodically;
- After cruiser service, specifically including transmission work or new tires;
- Via Speed Measurement Technology; or
- Via GPS Technology.

Speed Measurement Accountability

The Station/Unit Commander or designee shall maintain an inventory of all speed measuring devices under their control.

The inventory shall include:

- Serial number of all devices and associated equipment;
- The Department Inventory Control Number;
- Member assigned the device; and
- Spare devices that are unassigned.

Tracking History

Members should utilize the practice of Tracking History when conducting speed measurement and avoid independent reliance on the device.

Tracking history varies slightly on each type of device used but generally consists of:

- Identification of target vehicle;
- Estimation of Speed of target vehicle;
- Estimation of Range in feet when measurement taken;
- Check Environment for anything that could affect results;
- Pitch;
- Clarity;
- Steady Readout; and
- Consistent with visual estimate.

Limitations

The effective use of speed measuring devices and their acceptance by the public and courts is dependent upon the member's:

- Understanding the factors that limit the effectiveness of the device;
- Appropriate training and certification; and
- Proper care and use of the equipment.

Subject	Number
Speed Measuring Devices	**TRF-16**

References

Commonwealth v. Whynaught, 377 Mass. 19 (1979);
Commonwealth v El-Bayeh, Mass. (2020);
Honeycutt v Kentucky, (November 4, 1966) 408 SW2d 42;
NHTSA Speed Measurement Device Operator Training Manual 9/2018;
MPAC: 61.1.9.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

2259

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**TRF-17**
Subject:	
Emergency Roadblocks	

Policy

Situations may arise which necessitate the utilization of an emergency roadblock. To ensure the safety of the public and Department members, many factors have to be considered prior to implementation of a roadblock.

Only Commissioned Officers may approve and authorize the implementation of an emergency roadblock.

Definitions

Roadblock: A deliberate obstruction by physical means at one or more selected points on a roadway.

Activation and Implementation

Many factors need to be considered before the implementation of a roadblock. The decision to use a roadblock shall be based upon:

- The seriousness of the known or alleged crime;
- The number of members available to be assigned;
- The sufficiency of information and descriptions of wanted persons and vehicles;
- The elapsed time between the known or alleged criminal act and the time of reporting to the Department or other law enforcement agencies; and
- Any other pertinent facts.

Upon implementation of an emergency roadblock:

- A Patrol Supervisor shall be dispatched and shall assume command at the scene of the roadblock; and
- If available, the Air Wing should provide assistance.

Fixed Roadblocks

Fixed roadblock barricades may consist of any strong structure augmented by any combination of signs, signals, markers, reflectors, or flares, and may include the strategic positioning of cruisers on the roadway.

- No member shall remain in a cruiser utilized as a fixed roadblock; and
- Firearms may be made ready for use.

Circle System

The Circle System is designed to completely contain the suspect in a given area by blocking every possible avenue of escape.

Typically two (2) circles are established; an inner circle and an outer circle. The radius of the circles is determined by the estimated time that has elapsed from the commission of the crime. The locations of blocking points are then determined by using the crime scene as the center point and drawing circles around that point.

- The inner circle is the area immediately surrounding the crime scene; and
- The outer circle is set up to apprehend the fugitive if they get through the inner circle.

Incident Commanders/Supervisors shall assign members to:

- Patrol the area between the two circles;
- Staff blocking points established at major intersections and highways;
- Stop all traffic and interview each operator; and
- Use cover-contact techniques as appropriate.

Observation Techniques

It may be more desirable to slow traffic in order to enable members to check vehicles and occupants without bringing traffic to a complete stop.

Department vehicles should be parked at forty-five (45) degree angles with the traffic flow. In this position members can observe traffic and maintain mobility.

Blocking Two-Lane Roads

To stop traffic traveling in only one direction, Department vehicles should be:

- Parked at a forty-five (45) degree angle with the traffic flow;
- Partially on the roadway; and
- Blocking the lane to be stopped.

Light traffic can be stopped in both directions with this system. However, in heavy traffic it may be necessary to set up this blocking method on both sides of the road. This second roadblock should be close enough, (i.e., approximately seventy-five (75) yards away) and in sight of the first roadblock.

If signs and other warning devices are used, consideration should be given to the sight and stopping distances and the need for the element of surprise.

Subject:	Number:
Emergency Roadblocks	**TRF-17**

Blocking Roads at Night

At night, the member assigned as the contact officer shall:

- Stay off the roadway and out of oncoming headlights;
- Wear safety vest or high visibility clothing;
- Ensure roadblock lighting does not blind oncoming motorists; and
- Use cover-contact techniques as appropriate.

Blocking Multi-Lane Roadways

The blockade procedure for one side of a multi-lane highway is basically the same as for a one or two lane roadway.

A major difference is in the placement of signs and other warning devices.

- Because of greater speeds, the signs should be placed further away from the cruisers to allow motorists time to stop safely;
- If used, at least two (2) signs should be placed on both sides of the roadway facing towards oncoming traffic; and
- Flares and other warning devices should be arranged to funnel traffic into one or more lanes.

Post Incident Documentation and Review

A written report detailing the incident and the tactics used will be completed by the on scene Patrol Supervisor. The report will be forwarded through channels to the Division of Field Services Commander for an Administrative Review.

References: MPAC: 41.2.3.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

2262

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**TRF-20**
Subject:	
Department Vehicle Crashes	

Policy

The Department shall document, within the Records Activity Management System (RAMS), all Department vehicle crashes in accordance with this policy.

The Department shall objectively investigate all vehicle crashes to ensure that each crash investigation reflects the Department's commitment to impartiality and integrity.

Definitions

Cruiser Crash: A motor vehicle crash involving any Department vehicle, or any vehicle assigned to Department personnel, including civilian personnel.

Damage to a Department Vehicle: Non-crash damage, e.g. broken window or vandalism to an unattended vehicle. This includes windshield damage incurred as a result of debris from an unidentified or natural source.

Registry of Motor Vehicle (RMV) Forms: Department operators shall:

- Identify themselves as operator number one; and
- List the operator's address as:
  Department of State Police
  470 Worcester Road
  Framingham, MA 01702; and
- The owner's name and address shall be listed in accordance with the vehicle's registration.

Note: When a crash involves more than one Department operator, the investigating supervisor shall determine the numerical designation of each operator, such as Operator Number One, Operator Number Two, and so on.

Type I Crash: A minor cruiser crash not meeting any of the conditions of a Type II crash.

Type II Crash: A vehicle crash involving:

- Any injury or fatality to any party; or
- The issuance of a citation/criminal complaint; or
- Estimated damage over $1000 to any vehicle or property due to a crash; or
- Any civilian employee operating a Department vehicle.

Damage to Department Vehicle

Employees discovering/incurring damage to their assigned Department vehicles shall:

- Notify the sub-station of jurisdiction and request an entry to be made into the Daily Administrative Journal (DAJ);
- Report the damage, as soon as practicable, to their immediate supervisor and the Fleet Administrator per ADM-19A Vehicle Use and Maintenance.

Note: Any damage to a vehicle caused by a person arrested or a person summonsed to court shall be reported to the Fleet Section, in order to collect restitution. The investigating officer shall document the damage and take out appropriate criminal charges.

Type I Procedure

Employee	Duties
Member Involved in Crash	*Preliminary Procedures* • Immediately report the crash to the sub-station of jurisdiction; • If the Department vehicle was damaged, and no crash occurred, have photographs taken (not necessarily at the scene); • Ensure queries of license and registration data are done through the Registry databases and take appropriate action as necessary (See Type II); • Complete and submit within RAMS, the SP 425 Preliminary Documentation of Cruiser Crash prior to the completion of tour of duty; and • Completed reports shall be reviewed by the member's Station/Unit Commander prior to submission to Troop/Section Major; and • Complete and mail the original Registry form CRA-23, to the Registry of Motor Vehicles (RMV) within five (5) days. *Completed Documentation* • Completed documentation shall include: o To/From reporting the circumstances, to include the date the Registry CRA-23 was forwarded to the RMV; o A copy of the Registry CRA-23; and o Troop Mechanic's report and photographs. • Completed documentation shall be forwarded to their Troop/Section Major within five (5) days.

Type I Procedure, continued

Employee	Duties
Desk Officer	• Document the crash within the DAJ as a Type I Cruiser Crash activity; and • Notify the Troop Duty Officer.
Troop Duty Officer of Jurisdiction	• Document the crash within the DAJ; • Authorize operator to document crash; or • Assign a supervisor to investigate, preferably of higher rank than the member involved, from the Division of Field Services. **Note: Whenever a supervisor is assigned to investigate a cruiser crash, Type II procedures shall be followed.**
Involved Member's Station/Unit Commander	• Shall review reports for accuracy and completeness prior to submission to the Troop/Section Major.
Troop/Section Major	*Preliminary Documentation* The Troop/Section Major of the involved member shall: • Review the SP 425 upon receipt or no later than one (1) business day following the crash; • Ensure the Cruiser Crash is reclassified within RAMS from a Type I to a Type II if warranted; • Consult with the Major of jurisdiction within the Division of Field Services, to assign a supervisor to conduct a Type II Investigation when so determined; • Ensure that only a supervisor shall issue any citations related to the cruiser crash. *Completed Documentation* Upon receipt of all documentation the Troop/Section Major shall within RAMS: • Fill out the appropriate section of the SP 377; • Make findings and recommendations; and • Forward all documentation to the involved member's Division Commander within twenty-one (21) days of the crash.

Crash in Personal Vehicle

On-duty Department employees involved in a crash while operating their personal vehicles shall immediately inform their duty assignment supervisor of the crash when:

- They are authorized to operate their personal vehicle within the scope of their duties; and
- They are entitled to mileage pay for that travel.

Within five (5) days of the crash, the employee shall provide their duty assignment supervisor with a copy of the RMV CRA-23 and all other pertinent documentation and forward a copy to the Legal Section.

When a Department employee is injured in a crash that meets the criteria listed above, the injury shall be investigated as an on-duty injury.

Type II Procedure

Employee	Duties
Employee Involved in Crash	• Immediately report the crash to the sub-station of jurisdiction; • Preserve the scene, if safety and traffic concerns allow; • Members shall not take any enforcement action except to prevent parties from unlawfully leaving; • Complete and mail the Registry CRA-23 to the RMV within five (5) days; • Ensure their Station/Unit Commander has reviewed completed reports prior to submission; and • Complete and forward the following printed reports to the investigating officer within five (5) days (unless incapacitated): o To/From reporting the circumstances, to include the date the Registry CRA-23 was forwarded to the RMV; o A copy of Registry CRA-23; and o Commonwealth's Form 1 Notice of Injury (if injured).
Desk Officer	• Document the crash within the DAJ as a Type II Cruiser Crash activity; and • Notify the Troop Duty Officer.

Type II Procedure, continued

Employee	Duties
Troop Duty Officer of Jurisdiction	• Document the crash within the DAJ; • Assign a supervisor from within the troop to investigate, preferably of higher rank than the member involved. • If appropriate, notify the involved employee's Troop/Section Major or designee; and • Make arrangements for other assistance at the scene (Photographs, crash reconstruction, etc.).

Investigating Supervisor	*Preliminary Investigation*
	• Take command of the crash scene and investigation;
	• Have photographs taken of the scene and/or the damage;
	• Ensure queries of license and registration data are done through the Registry databases;
	• Take appropriate action on violations of law (e.g. citations);
	• Complete and submit the SP 425 within RAMS, prior to the completion of tour of duty; and
	• Complete and forward SP 624 Initial Injury Report if necessary. (Refer to ADM-11B Injury Reporting)
	
	Completed Investigation
	Forward reports to Troop Commander within fifteen (15) days from the date of the crash:
	• Registry CRA-65;
	• SP 209 Supplementary Cruiser Crash Report;
	• Troop Mechanic's Report and photographs of damage;
	• If applicable, towing bills;
	• If applicable, the SP 37 Statement In Support of Claim, Section 8;
	• All other reports, photographs, copies of citations, etc; and
	• If employee is incapacitated complete:
	  ○ SP 37 Sections, 1-7, and
	  ○ Commonwealth's Form 1.

Type II Procedure, continued

Employee	Duties
Involved Member's Station/Unit Commander	Shall review reports for accuracy and completeness prior to submission to the investigating supervisor.
Troop Commander of Crash Jurisdiction	*Preliminary Investigation* The Troop Commander shall: • Review the SP 425 upon receipt or no later than one (1) business day following the crash. *Completed Investigation* The Troop Commander shall within RAMS: • Make findings and recommendations; • If applicable, fill out the appropriate sections of the SP 37; • If applicable, fill out the appropriate sections of the SP 377 in RAMS; • Send a copy of the SP 37 and Commonwealth's Form 1 to Occupational Health if appropriate; and • Forward the completed report to the involved member's Division Commander within twenty-one (21) days of the crash.

Involved Employee's Division Commander

Division Commanders shall:
- Review all Type I and II reports including findings and recommendations;
- Complete appropriate sections of SP 377 in RAMS;
- Take corrective action when appropriate;
- Submit completed reports to the Division of Standards and Training within thirty (30) days of the crash; and
- Send a copy of the completed reports to the Fleet Section.

Division of Standards and Training

The Division of Standards and Training Commander or designee, shall:
- Complete appropriate section of SP 377 in RAMS;
- Ensure reports are complete and are filed within the Records Section; and
- If reports are not complete, return to the Division Commander for reconciliation.

The Commanding Officer or designee, of the Emergency Vehicle Operation Center (EVOC) shall within RAMS:
- Fill out and submit the appropriate section of the SP 377 when remedial training is completed.

Records Section The Records Section shall maintain all copies of reports and investigations upon receipt from the Division of Standards and Training.

References

SP 37 Statement in Support of Claim;
SP 209 Department Supplementary Cruiser Crash Report;
SP 377 Cruiser Crash Review Form;
SP 425 Preliminary Investigation of Cruiser Crash;
CRA-23 Motor Vehicle Crash Operator Report;
CRA-65 Motor Vehicle Crash Police Report;
Commonwealth's Form 1 Notice Of Injury.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**TRF-21**
Subject:	
Tire Deflation Devices	

Policy

The Department may use tire deflation devices in specific circumstances to reduce the speed and duration of pursuits in order to reduce the risk of injury to persons and/or damage to property.

Definitions

Channelizing: A technique where objects are placed in the anticipated path of a pursued vehicle in order to alter its direction.

Tire Deflation Device: A device that, when driven over, causes one or more tires of a vehicle to safely deflate.

Utilization of Tire Deflation Devices

Tire Deflation Devices shall:

- Be readily accessible;
- Only be deployed by a member trained in its use;
- Only be deployed if the device has a recovery cord; and
- Not be used to stop a motorcycle, moped, motorized scooter, tractor trailer, bus carrying passengers, or vehicle with less than four (4) wheels unless:
    - The suspect and/or vehicle poses an imminent threat of death or serious bodily harm to the public or officers; or
    - When specifically authorized and ordered by the Troop Duty Officer, Troop Commander or a Sworn Command Staff Member.

Site Selection

Tire deflation devices should not be used at intersections or in locations where geographic configurations (such as curves and steep embankments) increase the risk of injury to the suspect or occupants of other vehicles.

Deployment Notification

A tire deflation device should only be deployed when:

- The pursuing member has been informed of the location of deployment; and
- Has acknowledged this information on the radio.

Subject: Tire Deflation Devices	Number: TRF-21

Covert Deployment

Situations where it is prudent to covertly disable a vehicle with a tire deflation device may include:

- Stolen vehicles;
- Serious felony arrest warrants and/or charges; and
- Hostage or kidnapping situations.

Recovery of Tire Deflation Device(s)

A deployed tire deflation device(s) shall be safely removed from the roadway after the fleeing vehicle passes. Members shall not enter into the travel lane until all traffic is clear and it is safe to retrieve the device from the roadway. The deployed device(s) shall not be left unattended in the roadway.

Duty of Pursuit Member(s)

On approach to the deployment area the pursuing member(s) shall proceed cautiously and adjust the cruiser speed as necessary to:

- Allow time for the removal of the tire deflation device; or
- Respond to sudden evasive or unpredictable maneuvers by the fleeing vehicle.

After clearing the deployment area, member(s) may increase cruiser speed, as necessary.

Reporting

Members shall report all deployments:

- To the Troop Duty Officer of jurisdiction; and
- To the Emergency Vehicle Operations Center (EVOC) via SP 601 Tire Deflation Device Evaluation Form.

Members shall also complete a supplemental report detailing the incident and tactics utilized in the deployment.

The Troop Duty Officer shall report the use of a tire deflation device and the results in the Daily Administrative Journal (DAJ) and in the electronic RAMS Pursuit Evaluation.

Maintenance of Tire Deflation Device

Members assigned tire deflation devices shall maintain them according to the manufacturer's guidelines and specifications.

Non-functioning parts/units shall be forwarded to the EVOC Coordinator for replacement, unless otherwise indicated.

Subject:	Number:
Tire Deflation Devices	**TRF-21**

Damage to Vehicles or Property

The Troop Duty Officer shall assign a supervisor to investigate any related damage to any other vehicle or property.

Third party owners of any damaged vehicle or property shall be advised to contact the Legal Section for guidance in filing a claim at (508) 820-2311.

References: TRF-04 Motor Vehicle Pursuits;
SP 601 Tire Deflation Device Evaluation Form;
RAMS Pursuit Evaluation;
MPAC: 41.2.3.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
July 22, 2022	**TRF-22**
Subject: **Escorts, Relays and VIP/Dignitary Security**	

Policy

The Department may authorize escorts or relays to provide added security, expedite the delivery of special items, and ensure the safe and efficient movement of traffic.

General Guidelines

The Division of Field Services Commanding Officer shall have operational control of all escorts and relays.

Routine requests for escort or relay services shall be approved as outlined below. All emergency requests for escort or relay services shall be forwarded to the Troop Duty Officer.

Members shall not initiate or commence any escort or relay without permission from the Troop Duty Officer.

Routine Requests

If the request is for…	**Then the request should be forwarded to…**
• Any subdivision of the United States Government; • Executive Security; • Political or high-profile figures; or • Nuclear, radiological, biological, hazardous, and/or sensitive materials.	Troop "S" Commanding Officer or designee.
• Funerals, parades, etc.; • Public safety vehicles; or • Other instances where an escort or relay is in the public interest.	Troop Commander or designee.
• Oversize vehicles; or • Unusual cargo.	Troop Detail Officer

Routine Requests, continued

Whenever possible, the request shall be in writing and include the trip route and any other pertinent information. Notification of an escort or relay shall be made to any affected Troop.

Emergency Requests

Legitimate requests for unscheduled Department escort or relay services may include:

- Protection of life;
- Medical personnel;
- Exigent medical need;
- Other law enforcement agencies; or
- Valuable cargo, which may include blood, life-saving medicines, human organs and tissues, or other materials as required by law.

The Troop Duty Officer shall notify the GHQ Communications Section of every escort or relay that extends beyond the Troop area.

Emergency escort of ambulances or private vehicles should be avoided except when a life is in jeopardy or under exigent circumstances. Permission to escort shall be sought immediately from the Troop Duty Officer.

Escort of Nuclear, Radiological, Biological and/or Sensitive Materials

The movement of nuclear, radiological, biological and/or other sensitive materials in and through the Commonwealth may require the utilization of an escort.

When an escort is recommended by the Massachusetts Department of Public Health, the Commanding Officer of Troop "S" or his/her designee shall develop an Operations Plan that will ensure the following steps are undertaken:

- Notify the Division Commander of Field Services;
- Notify the Division Commander of Homeland Security and Preparedness;
- Notify the Division Commander of Investigative Services;
- Notify the Emergency Management Unit;
- Assign a Commissioned Officer from Special Operations as the escort Incident Commander / OIC;
- Ensure that Commercial Vehicle Enforcement Section (CVES) personnel provide appropriate inspections of the vehicle(s) to be escorted. CVES personnel will accompany the escort for the duration of the escort;
- Contact the Division Commander of Homeland Security and Preparedness to request a dedicated Air Wing unit to provide aerial surveillance for the duration of the escort if deemed necessary;
- Assign Special Tactical Operations (STOP) Team personnel to coordinate appropriate security measures. STOP Team personnel will, as appropriate, utilize armored or other assigned vehicles during the escort;

Escort of Nuclear, Radiological, Biological and/or Sensitive Materials, continued

- Assign the Motorcycle Unit, as appropriate, to facilitate the movement of the escort; and
- Assign other Special Operations assets as appropriate.

The Emergency Management Unit shall coordinate the escort with the following entities, as appropriate:

- Special Operations Commanding Officer;
- CVES;
- Air Wing;
- STOP Team;
- Motorcycle Unit;
- Criminal Information and Intelligence Section - Commonwealth Fusion Center;
- Troop Commanders of each Troop through which the escort will travel;
- Communications Section;
- Fiscal Section;
- State Police agency for adjoining state(s) through which the escort will travel;
- Police department of the receiving/departing community;
- Police department of adjoining communities, as appropriate;
- Massachusetts Department of Public Health Radiation Control Program;
- Shipping/receiving company; responsible financial party; and
- Additional notifications, as appropriate.

The Criminal Information and Intelligence Section Commanding Officer, or his/her designee, shall assign personnel to:

- Conduct open source research related to the shipment;
- Query internal databases to determine if the Commonwealth Fusion Center has any relevant information pertaining to the shipment;
- Contact a representative of the U.S. Department of Homeland Security's Intelligence and Analysis Section to determine if DHS has any relevant information pertaining to the shipment;
- Contact a representative of the Federal Bureau of Investigation's Boston Field Office to determine if the FBI has any relevant information pertaining to the shipment;
- Contact a representative of the Boston Regional Intelligence Center to determine if the BRIC has any relevant information pertaining to the shipment; and
- Report all results and significant findings to the Emergency Management Unit's Commanding Officer.

Troop Commanders of each Troop through which the escort travels shall:

- Provide notification to communities, as appropriate; and
- Provide uniformed personnel, as appropriate, to facilitate the movement of the escort through the Troop.

Communications Section shall:

- Assign a SOPs channel for escort personnel to utilize.

Escort of VIP or Dignitary

The movement of political or high-profile figures, in and through the Commonwealth, may require the utilization of an escort.

When a VIP or dignitary escort is requested and authorized, the Commanding Officer of Troop "S" or his/her designee shall develop an Operations Plan that will ensure the following steps are undertaken when applicable:

- Notify the Division Commander of Field Services;
- Notify the Division Commander of Homeland Security and Preparedness;
- Notify the Division Commander of Investigative Services;
- Notify the Emergency Management Unit;
- Assign a Commissioned Officer from Special Operations as the escort Incident Commander / OIC;
- Contact the Division Commander of Homeland Security and Preparedness to request a dedicated Air Wing unit to provide aerial surveillance for the duration of the escort if deemed necessary;
- Assign Special Tactical Operations Team personnel to coordinate appropriate security measures. STOP Team personnel will, as appropriate, utilize armored or other assigned vehicles during the escort;
- Assign the Motorcycle Unit, as appropriate, to facilitate the movement of the escort; and
- Assign other Special Operations assets as appropriate.

The Special Operations Commander or Designee shall coordinate the escort with the following entities, as appropriate:

- Special Operations Commanding Officer in charge of escort/relay;
- Air Wing;
- STOP Team;
- Motorcycle Unit;
- Criminal Information and Intelligence Section-Commonwealth Fusion Center;
- Troop Commanders of each Troop through which the escort will travel;
- Communications Section;
- Fiscal Section;
- State Police agency for adjoining state(s) through which the escort will travel;
- Police department of the receiving/departing community;
- Police department of adjoining communities, as appropriate; and
- Additional notifications, as appropriate.

Troop Commanders of each Troop through which the escort travels shall:

- Provide notification to communities, as appropriate; and
- Provide uniformed personnel, as appropriate, to facilitate the movement of the escort through the Troop.

Communications Section shall:
Assign a SOPs channel for escort personnel to utilize.

Subject: Escorts, Relays and VIP/Dignitary Security	Number: TRF-22

Escort Request for Charitable Events

At least thirty (30) days in advance, organizers of a legitimate charity shall provide the Paid Detail Officer of jurisdiction a written plan and sign a SP 618 Motorcycle Escort Waiver. The Troop Major may allow exceptions to the thirty-day notice under extraordinary circumstances.

The written plan shall contain:

- The date of the event, routes of travel, and the anticipated number of participants;
- Number of Department members requested for escort;
- Notification to local and state authorities, and media in writing;
- Proof of the required one million dollar bond to cover the event; and
- Acknowledgement that participants shall obey all traffic laws during the duration of the event.

Outlaw Motorcycle/ Criminal Gangs

The Paid Detail Officer shall consult with the Criminal Information and Intelligence Section if it appears that the event organizers, or likely participants, have any association with criminal activity.

Outlaw motorcycle/criminal gangs shall be barred from obtaining Department escorts.

References

ADM-25 Paid Details;
TOP-01 Special Operations Command and Control;
SP 618 Motorcycle Escort Waiver;
MPAC: 46.2.6, 61.3.3.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**TRN-01**
Subject:	
Training Administration	

Policy

The Department shall provide training that will develop the skills necessary for the safe, professional and effective performance of its personnel, and that is designed to promote and maintain the professionalism and operational readiness of the Department.

The Department shall ensure that all employees successfully complete compulsory training and annual in-service training as required by law and the Colonel/Superintendent.

The Department shall provide documented training related to the roles and responsibilities of promoted sworn members and civilian employees promoted to supervisory roles.

State Police Academy

The State Police Academy is commanded by the Deputy Division Commander of Standards and Training, who is responsible for ensuring that all training is conducted in accordance with Department directives and applicable laws.

Academy Staff Responsibilities

The Academy Staff shall:

- Identify, develop, and evaluate training and educational programs;
- Assist in the development of lesson plans for all Department training courses;
- Provide necessary training to Department employees and the law enforcement community;
- Meet all federal, state and Department mandated training requirements;
- Provide training to develop the skills necessary for the safe, professional and effective performance of its employees;
- Provide career development opportunities for employees; and
- Maintain training records for employees, including attendance records.

Lesson Plans

- Lesson plans are required for all training courses conducted by the Department;
- Lesson plans shall include, at a minimum:
  - A statement of performance and job-related objectives;
  - The content of the training and specifications of the instructional techniques; and
  - Identification of tests related to the instruction;
- Lesson plans shall be approved and signed/initialled by the Commandant of the Academy, or designee, prior to administration of the training; and

- Upon approval, lesson plans developed by Department members shall remain the intellectual property of the Massachusetts State Police.

Attending Training

Employees assigned to all training programs shall:

- Report at the specified time and location with the proper uniform/attire and materials;
- Be returned to their duty assignment for failing to report as directed and may be subject to disciplinary action;
  - Employees with a scheduling conflict due to court or approved time off shall notify their first line supervisor to request to reschedule the training; and
- Attend non-mandatory training programs only as approved in accordance with Departmental guidelines.

Note: Changes in work schedules for the purpose of training shall be in accordance with the Collective Bargaining Agreement.

Training Requests

Massachusetts State Police personnel requesting to attend a training program that has *any* costs associated with it and/or is held outside of the Department shall comply with the following:

- ***At least forty-five (45) days prior*** to the anticipated date of the requested training, ***each traveler*** shall refer to the Travel/Training Guide, located in the State Police Document Management System, and electronically submit, through channels to their Division Commander:
  - A To/From requesting approval;
  - A completed *SP 371 Travel Training Endorsement Sheet;*
  - A completed *Commonwealth of Massachusetts Travel Authorization Form* (TAF Form Primary);
    1. ***NOTE***: *Section 9 "Travel Itinerary and Justification*" must include a ***thorough*** explanation of how the training will benefit the Commonwealth;
    2. ***NOTE***: *Section 10 "Expenses"* must be completed even if the cost of the Travel/Training will be paid by personal funds, Commonwealth funds, or federal/ Other State Funds;
  - If the travel and/or training is funded by a private entity, a completed *Disclosure by Non-Elected Public Employee of Travel Expenses Serving a Legitimate Public Purpose* form;
    1. ***NOTE:*** Each traveler must estimate and account for expenses in the "Itemization and explanation of amounts offered" section when travel/training is funded by a private entity; and
  - **All** supporting documentation (i.e. training fees and agenda; lodging and transportation estimates; meal reimbursement rates and other appropriate expenses as specified in the member's appropriate Collective Bargaining Agreement.)

- When estimating expenses, it is the responsibility of the traveler to ascertain and account for taxes and fees associated with hotel reservations, car rentals, etc. It is also the responsibility of the traveler to minimize all costs associated with travel and training.

Training Requests, continued

- If the training is out-of-state, personnel should review on PowerDMS the Executive Office of Administration and Finance *Out Of State Travel Guidelines.*

The Division Commander, or designee, within five (5) days of receipt of the training request shall forward approved requests and accompanying documentation to:

- The Deputy Superintendent; and
- The Department's Leave Coordinator per ADM-11E Leaves of Absence.

State Police Academy Coordinated/ No Cost Training

Massachusetts State Police personnel requesting to attend training that is coordinated by the State Police Academy and has no costs associated with it **need not** submit To/From and travel forms as described in the previous section. Instead, personnel interested in attending such training shall complete the *MSP Professional Development Registration* form which will be attached to the State Police Academy e-mail that announces such training. Personnel shall submit the **completed** registration form to the State Police Academy.

Expense Reimbursement

Reimbursement for expenses shall be made only if prior written approval has been received from the Deputy Superintendent.

In order to be reimbursed for expenses, *each* traveler must submit to the Fiscal Section a completed *Employee Travel/Training/ Reimbursement Voucher Input Form* along with all necessary receipts and paperwork.
Note: The reimbursement amount should not exceed the previously authorized expenditure.

Testing

Instructors shall use competency based testing with performance objectives designed to measure the participant's ability and knowledge of course related skills. Participants shall be advised of minimum acceptable standards prior to the administration of such tests.

Remedial Training

Employees who fail to meet required standards of performance shall be required to participate in documented remedial training, as soon as possible.

The goal of remedial training is to ensure that employees demonstrate the knowledge, ability, and skills to achieve an acceptable level of performance.

Employees, who fail to attend assigned remedial training, and/or who fail to achieve acceptable levels of performance, shall be subject to disciplinary action.

Records

In order for the Department to maintain complete and accurate training records, commencing January 1, 2012, members shall:

- Forward copies of training certificates or records of attendance for non-Department training to:
  - The State Police Academy (SPA); and
  - Their Station/Section/Unit Commanding Officer.
- Ensure that copies of certificates or records of attendance for any future non-Department trainings are forwarded to:
  - The State Police Academy (SPA); and
  - Their Station/Section/Unit Commanding Officer.

Note: If available, members are encouraged to forward training records acquired before January 1, 2012, to their Commanding Officer and the SPA for insertion into their Individual Training files.

Station/Section/Unit Commanding Officers shall:

- Ensure that all members under their command have an Individual Training File that is retained and updated within the Station/Section/Unit; and
- Ensure that the Individual Training File is administratively forwarded together with the member's Attendance Calendar(s) and the Employee Evaluation System (EES) Fact File when, transferred out of the Station/Section/Unit.

The Academy Commandant shall be responsible for maintaining current Department training records. Such records shall include, but not be limited to:

- Name, rank, ID#, and duty assignment of Department employees attending all training programs;
- Name and agency of non-department personnel attending all training programs;
- Attendance records;
- Name of instructor and course lesson plan;
- Individual records of performance evaluations administered with associated results; and
- The type of certificates, received, if any

All lesson plans, attendance records and testing results are filed and retained indefinitely.

Training for Civilian Employees

In Accordance with TRN-04 Professional Development, the Director of Human Resources shall develop and maintain guidelines related to the training and education of civilian employees.

All newly appointed civilian employees shall receive training in the following areas, at a minimum:

- Mission, goals and objectives of the Department;
- Applicable Department policy, procedure, rules, regulations and guidelines (e.g. workplace violence, harassment);
- Department Accreditation program/process;
- Department expectations and the civilian employees performance evaluation program;
- Working conditions of hired position; and
- Responsibilities and rights of employees.

Civilian positions requiring pre-service and in-service training shall be identified by the Director of Human Resources.

The Department shall provide training to civilian employees in accordance with law, Department policy and as requested by the Director of Human Resources. The Academy shall coordinate the presentation of training to civilian employees, as requested by the Director of Human Resources.

References:

ADM-11E Leaves of Absence;
TRN-04 Professional Development;
SP 371 Travel Training Endorsement Sheet;
Commonwealth of Massachusetts Travel Authorization Form (TAF Form Primary);
Disclosure by Non-Elected Public Employee of Travel Expenses Serving a Legitimate Public Purpose form;
Executive Office of Administration and Finance Out Of State Travel Guidelines;
MPAC: 33.1.1, 33.1.2, 33.1.3, 33.2.1, 33.3.1, 33.3.2, 33.5.1, 33.7.1, 33.7.2, 33.8.2.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**TRN-02**

Subject:

Recruit Training

Policy

Prior to assuming duties as a sworn State Police Trooper, recruits shall be assigned to, and satisfactorily complete, a recruit training class. This class shall be held at the State Police Academy and fulfill the requirements as prescribed by Massachusetts General Laws and the Colonel/Superintendent.

Recruit Handbook

The Academy Commandant shall, prior to the commencement of a recruit training class, prepare and distribute to each recruit a handbook containing the following information:

- Recruit performance expectations;
- The rules and regulations governing the conduct of recruits while assigned to the Academy; and
- The method for determining the final overall average score of each recruit which shall be used to establish the class standing of each trainee.

Recruit Class Curriculum

The Academy Commandant shall develop a recruit class curriculum including, but not limited to:

- Constitutional principles, criminal law and procedure, motor vehicle law;
- Department operations, Rules and Regulations, Policies and Procedures;
- Use of force, including firearms;
- Emergency vehicle operations;
- CPR/First Responder training;
- Principles of leadership;
- Report writing, court testimony and communications skills;
- Cultural diversity and ethics; and
- Physical fitness and wellness.

Authorized Use of Recruits

The Colonel/Superintendent may authorize the use of recruits assigned to the State Police Academy to tasks not requiring law enforcement powers.

References: MGL c.22C;
MPAC: 33.4.2.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**TRN-03**
Subject:	
Field Training Program	

Policy

The Department shall provide a Field Training Program for recent Recruit Training Troop (RTT) graduates to transition from the controlled learning environment of the Academy to the responsibilities and duties of a State Trooper.

Field Training Program

The Field Training Program shall be twelve weeks in duration, or as prescribed by the Colonel/Superintendent. Successful completion of the program is contingent upon satisfactory attendance and performance.

Probationary Troopers may be assigned to three (3) Field Training Officers (FTOs), on different shifts, as set forth in the Field Training Program. Exceptions may be made for specific operational and training reasons.

Excessive absenteeism shall be reported to the Field Training Administrator and may result in termination of the Probationary Trooper.

Academy Commandant

The Academy Commandant is responsible for the administration of the Field Training Program. The Academy Commandant shall coordinate the selection of an appropriate number of FTOs through the Division of Field Services.

Prior to the commencement of the Field Training Program, the Academy Commandant shall develop and provide training to Station Commanders and FTOs. This training shall, at a minimum:

- Provide an overview of the current Academy recruit training program reinforcing:
  - The mission of the Department;
  - Fundamental training values;
  - Department goals and objectives; and
  - Instructions on the administration and reporting requirements of the Field Training Program.

Subject: Field Training Program	Number: TRN-03

Field Training Administrator

The Academy Commandant shall designate a member of the Academy Staff as the Field Training Administrator. The Field Training Administrator shall be responsible for:

- The management of the Field Training Program;
- The development and distribution of the Field Training Program Manual; and
- Coordinating the selection of FTOs with Troop Field Training Coordinators.

Troop Commander

The Troop Commander shall:

- Appoint a member to serve as the Troop Field Training Coordinator; and
- Allow the Troop Field Training Coordinator to modify their work schedule to effectively manage the Field Training Program.

Troop Field Training Coordinator

The Troop Field Training Coordinator shall:

- Administer the Field Training Program;
- Act as the liaison with the Field Training Administrator; and
- Review the Daily/Weekly Observation Reports on a weekly basis.

Station Commander

Station Commanders shall:

- Administer the Field Training Program within their sub-station;
- Review and approve all submitted FTO evaluations;
- Forward the approved evaluations to the Troop Field Training Coordinator; and
- Immediately notify the Troop Field Training Coordinator of any issues that arise during the Field Training Program.

Field Training Officer

The FTO performs a critical role in the development of the new trooper and shall be responsible for:

- Providing an effective learning environment through leadership and experience;
- Providing an opportunity to realistically apply the knowledge, ability, and skills acquired during academy training;
- Providing an example that promotes professionalism, public respect, and confidence;
- Complying with the procedures established in the Field Training Program; and
- Assessing the performance of Probationary Troopers and providing remedial instruction as necessary.

FTO's shall receive training in the FTO program both upon initial FTO assignment and subsequently prior to the graduation of any RTT for which the member will be assigned as an FTO.

Subject:	Number:
Field Training Program	**TRN-03**

Field Training Program Manual

The Field Training Program Manual shall:

- Be provided to Station Commanders and FTOs prior to the commencement of the Field Training Program;
- Clearly define the responsibilities of the FTO; and
- Provide specific direction concerning the knowledge, ability, and skills to be taught, performed and assessed.

Selection Process

The identification and selection of the FTOs is critical to the success of the Field Training Program.

Selection Process

- Station Commanders shall recommend to the Troop Commander members who demonstrate integrity, character, and commitment to the Field Training Program;
- Troop Commanders shall approve and forward the final list of FTOs to the Commander of the Division of Field Services; and
- The Division of Field Services Commander shall forward the names of the approved FTOs to the Academy Commandant.

Evaluations

Station Commanders and FTOs shall ensure that all written evaluation forms are submitted in accordance with the Field Training Program Manual.

All deficiencies that may impact the ability of the Probationary Trooper to safely and successfully complete the Field Training Program shall be brought to the attention of the Station Commander immediately.

Completion of Program

After twelve (12) weeks, the Station Commander shall forward a recommendation to the Field Training Administrator which shall include a conclusion as to:

- The Probationary Trooper is capable of working on their own; or
- An extension of the Field Training Program is necessary; or
- Termination of employment is appropriate.

The Troop Commander shall forward all recommendations for termination to the Colonel/Superintendent, through channels after consultation with the:

- Field Training Officer(s);
- Station Commander;
- Troop Field Training Coordinator; and
- Field Training Administrator.

References: MPAC: 33.4.3

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**TRN-04**
Subject:	
Professional Development	

Policy

The Department recognizes the necessity of continuous education and training in order to maintain and enhance the knowledge, abilities, and skills of its sworn and civilian employees.

This shall be accomplished, in part, through an ongoing professional development program to include annual in-service training.

Compulsory Training

The Department shall provide compulsory training to all members.

The Deputy Division Commander of Standards and Training, shall:

- Ensure that an annual training assessment is conducted to identify the training and educational needs of the Department;
- Ensure the Academy Staff develops a training curriculum, based on annual training assessment; and
- Forward the training curriculum, through channels, for review and approval by the Colonel/Superintendent.

Members shall attend/receive compulsory training annually on dates assigned. Members who fail to attend may be subject to discipline.

In-service training may be conducted at the State Police Academy, any site approved by the Colonel/Superintendent, or through approved alternative means of communicating essential training/information to Department members.

Online Academy

The Online Academy Unit within the Academy shall:

- Be responsible for the development and distribution of online training, including, but not limited to, legal updates.

Members are encouraged to submit recommendations for training topics to the Online Academy Unit.

Subject:	Number:
Professional Development	**TRN-04**

Professional Development

The Department shall identify and develop training programs to be presented internally which shall provide its sworn and civilian employees with the opportunity to expand or enhance their knowledge, abilities, and skills in specialized areas, or upon promotion.

The Academy Staff shall be responsible for:

- Development and/or administration of courses in accordance with the procedures outlined in TRN-01 Training Administration;
- Maintaining a current schedule of professional development courses on the intranet website;
- Maintaining accurate attendance records for members who have attended training; and
- Forwarding to respective Troop/Section Commanders the accurate attendance records for members who have attended training upon completion of training.

Lesson plans, attendance records and grades shall be maintained indefinitely

Sworn and civilian employees may attend trainings or seminars intended to improve their professional abilities. Sworn and civilian employees requesting to attend professional development courses shall adhere to the procedure outlined within TRN-01 Training Administration. Authorization to attend may be granted based upon the applicability of the program and available Department resources.

Training Records

For the Department to maintain complete and accurate training records, commencing, January 1, 2012, members shall:

- Forward copies of training certificates or record of attendance for non-Department training to:
  - The State Police Academy (SPA); and
  - Their Station/Section/Unit Commanding Officer.
- Ensure that copies of certificates or records of attendance for any future non-Department trainings are forwarded to:
  - The State Police Academy (SPA); and
  - Their Station/Section/Unit Commanding Officer.

Note: If available, members are encouraged to forward training records acquired before January 1, 2012, to their Commanding Officer and the SPA for insertion into their files.

Station/Section/Unit Commanding Officers shall:

- Ensure that all members under their command have an Individual Training File that is retained and updated within the Station/Section/Unit; and
- Ensure that the Individual Training File is administratively forwarded together with the member's Attendance Calendar and the Employee Evaluation System (EES) Fact File when transferred out of the Station/Section/Unit.

Subject: Professional Development	Number: TRN-04

Training for Civilian Employees

The Director of Human Resources shall develop and maintain guidelines related to the training and education of civilian employees.

All newly appointed civilian employees shall receive training in the following areas, at a minimum:

- Mission, goals and objectives of the Department;
- Applicable Department policy, procedure, rules, regulations and guidelines (e.g. workplace violence, harassment);
- Department Accreditation program/process;
- Department expectations and the civilian employees performance evaluation program;
- Working conditions of hired position; and
- Responsibilities and rights of employees.

The Department shall provide training to civilian employees in accordance with law, Department policy and as requested by the Director of Human Resources. The Academy shall coordinate the presentation of training to civilian employees, as requested by the Director of Human Resources.

References: TRN-01 Training Administration;
MPAC: 33.1.2, 33.5.1, 33.7.1, 33.7.2, 33.8.3.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 22, 2022	**TRN-05**
Subject:	
State Police Cadet Program	

Policy

In accordance with M.G.L. c. 22C, § 10A the Colonel/Superintendent has established a State Police Cadet Program within the Department. The Program consists of a selection process for each Cadet Class, training at the State Police Academy, in-service training, and a series of rotating work assignments for a minimum of one year. Upon successful completion of the Program and passage of the Civil Service entrance examination, State Police Cadets may receive appointment to a Recruit Training Troop.

Purpose

To attract qualified candidates to a career in law enforcement, expose them to the operations and objectives of the Department, and encourage them to pursue a position as a Massachusetts State Police Trooper.

Goal

The underlying objectives of the Cadet Program are to provide young women and men with an alternative pathway to become sworn members of the Massachusetts State Police, as well as to increase recruitment, retention, and enhance diversity of personnel within the Department.

Cadet Academy and Training

The Academy Commandant shall develop a Cadet Class curriculum that will provide training related to the subject matter and skills utilized by the Department. The Academy Commandant determines the minimum acceptable standards for the Cadet Class as approved by the Colonel/Superintendent.

Cadets shall receive in-service training throughout the duration of the Cadet Program as determined by the Cadet Program Coordinator.

Cadet Training and Field Manual

Prior to the commencement of a Cadet Class, the Academy Commandant shall prepare and distribute to each Cadet a State Police Cadet Training and Field Manual containing, at a minimum, the following information:

- Cadet Academy performance and conduct expectations
- Cadet Standard Operating Procedures
- Cadet Code of Conduct / Cadet Rules of Conduct
- Cadet Program Policy

Cadet Program Directors

The State Police Cadet Program Directors shall consist of a Cadet Program Coordinator and a Cadet Program Administrator. The Cadet Program Coordinator shall be a commissioned officer and the Cadet Program Administrator shall be a civilian employee.

Duties

A Cadet is a civilian employee of the Department and shall not have any power of arrest other than that of an ordinary citizen. Cadets shall not carry firearms and/or any other use of force equipment.

Cadets may assist sworn members or civilian employees with any duties not requiring law enforcement powers as authorized by the Colonel/Superintendent.

Cadets may provide support to Department employees by performing administrative tasks, and providing supplemental aid as directed and assigned during operations and special occasions. Examples of such occasions include, but are not limited to, rendering non-sworn assistance during search and rescue missions, serving as support during large-scale events, or helping with the agency response to public safety emergencies resulting from extreme inclement weather or criminal activity.

Cadets may be permitted to participate in a patrol observation at the discretion of the Station/Section/Unit Commander and participating sworn member.

Cadets shall not perform any operational functions pertaining to detainees to include, but not be limited to, booking of detainees, cell checks, suicide watch, searches, and escorts.

Cadets shall not be involved in the collection of evidence, whether physical or testimonial or the evidentiary chain of custody processes.

Work Rotations

Cadets shall be assigned to various work assignment rotations throughout the Department as approved by the Colonel/Superintendent.

The Cadet Program Directors shall coordinate with Division Commanders to determine appropriate work assignments, work schedules, and duration of assignments.

Work Schedule and Physical Fitness

Cadets shall be assigned to work an eight and one-half hour work shift including a thirty-minute unpaid meal period to be taken as close to the middle of the work shift as possible. Cadets are not permitted to work through their meal period in order to arrive late to or leave early from their work shift.

Cadets are expected to participate in health maintenance in keeping with established standards for State Police Cadets for no longer than one hour during their scheduled work shift.

Supervision and Evaluations	Cadets will be assigned to the Station/Section/Unit Commander or Civilian Manager of their assigned work rotation. Station/Section/Unit Commanders and Civilian Managers will be responsible for Cadet evaluations, which will subsequently be reviewed by the Cadet Program Directors. Utilizing the series of rotation evaluations, the Cadet Program Directors will complete semi-annual, and annual evaluations, as well as an overall evaluation for each Cadet at the end of his/her tenure with the Program. Cadets' weekly HR/CMS payroll will be reviewed and approved by the Cadet Program Directors. Dual notification is required for all time off requests. Cadets shall submit requests for time off to the Cadet Program Directors and shall notify their Station/Section/Unit Commander, Civilian Manager or their designee.
Responsibilities of Sworn and Civilian Personnel	Sworn and civilian personnel shall create a professional work environment for Cadets to learn the operations and objectives of their work assignments. Such an environment will be fostered by providing exposure to and demonstration of various job tasks, and by encouraging mentorship by sworn and civilian personnel for the Cadets. Sworn and civilian personnel may provide positive or negative observations regarding a Cadet's performance to the Cadet's assigned Station/Section Unit Commander and/or the Cadet Program Directors.
Adherence to Rules, Regulations, and Policies	Cadets shall adhere to all Rules and Regulations and Policies and Procedures as required for all civilian employees of the Department as well as any Rules, Regulations and/or Policies or written directives specifically applicable to Cadets. Cadets shall also adhere to the State Police Cadet Training Manual including Cadet Rules of Conduct and SOPs for Cadets.
Extended Leave of Absence	Cadets on any approved leave of absence to include but not limited to FMLA, Military Leave, and Injured on Duty shall have to extend their time as a Cadet to fulfill the minimum twelve (12) month requirement for the Cadet Program if the twelve (12) months has not already been met. Cadets on any extended leave of absence will be referred to the Cadet Review Board.
Drug Testing	Cadets will be subject to random, reasonable suspicion, and post-incident drug testing. Refer to Cadet Drug Testing SOP.

Cadet Review Board (CRB)

The five (5) member Board will meet on an as needed basis to consider and act on any Cadet disciplinary or job performance issues. The Board will make written recommendations to the Colonel regarding any Cadet disciplinary or employment issues.

- Three (3) Commissioned Officers, one (1) of which will be the Department's Diversity Officer
- One (1) Department Human Resources Section Representative
- One (1) Department Civilian Manager

The Board will be made up of appointed members, along with appointed alternates, in order to maintain member familiarity with the Cadet Program practices and precedent.

In addition to the five Board members, the Cadet Coordinator or their designee shall act as the Board Facilitator. The Facilitator will be responsible for obtaining all needed documentation, and arranging testimony, when necessary, for the board to properly render a decision regarding business before it.

All meeting minutes and actions of the board will be maintained in ACISS by a Commissioned Officer member of the board assigned as Secretary for that particular meeting of the Board.

One Commissioned Officer will be assigned as the President for each meeting of the Board for the purpose of presiding over the meeting and maintaining decorum, seeking input from members, seeking outcome proposals by members, and after a meeting of the Board, declaring the Board's findings.

The Board will meet quarterly or as needed.

Uniform

Cadets shall wear the issued uniform unless alternate attire authorized by Station/Section/Unit Commander or designee and approved by the Cadet Program Directors.

References: MGL c. 22C, § 10A

Promulgated By: Christopher S. Mason, Colonel/Superintendent

2293

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**UOF-01**
Subject:	
Use of Force	

Policy

Members are authorized to use only that force which is objectively reasonable, in accordance with all applicable federal and state laws and regulations and the contents of this policy to:

- Effect the lawful arrest or detention of an individual;
- Prevent the escape from custody of an individual; or
- Prevent imminent harm, and the amount of force used is proportionate to the threat of imminent harm.

Members should assess each situation to determine which action shall best bring the incident under control, using only that amount of force that is reasonably necessary.

Members are authorized to use deadly force in accordance with applicable federal and state laws and regulations and the contents of this policy in order to protect themselves or others from an immediate threat of death or serious bodily harm.

If feasible, some clear, verbal warning shall be given before any use of force (UOF). Such warning should include identifying the member as a law enforcement officer where it is not readily apparent (e.g., at night; member is in plainclothes; member is in an unmarked vehicle.)

Members ***shall not use*** a chokehold or other tactics that restrict or obstruct an individual's breathing or oxygen or blood flow to an individual's head or neck. Members shall not be trained to use a lateral vascular neck restraint, carotid restraint or other action that involves the placement of any part of the Member's body on or around an individual's neck in a manner that limits the individual's breathing or blood flow.

Except to temporarily gain, regain or maintain control of an individual and apply restraints, a Member ***shall not*** intentionally sit, kneel, or stand on an individual's chest, neck, or spine, and shall not force an individual to lie on their stomach.

A Member ***shall not*** obstruct the airway or limit the breathing of any individual, nor shall a Member restrict oxygen or blood flow to an individual's head or neck. An individual placed on their stomach during restraint should be moved into a recovery position or seated position as soon as possible.

Subject	Number
Use of Force	**UOF-01**

Policy, continued

When it is objectively reasonable that a subject is under the control of law enforcement, the UOF shall terminate.

When safe, and tactically feasible, members shall always provide appropriate medical response and proper medical aid to individuals who are exhibiting signs of, or complaining of, injury or illness, including following a UOF or other law enforcement action.

Definitions

Actively Resistant Individual: An individual who uses physical strength and/or body movement to resist a Department member. Examples of active resistance include pulling, turning, or walking away from an officer.

Aggravated Assaultive Individual (Serious Bodily Harm/Death): An individual who engages in conduct that is likely to produce death or serious bodily harm to a Department member or another individual.

Assaultive Individual (Bodily Harm): An individual who attempts to injure a Department member or another person or engages in conduct that has the potential to injure a Department member or another person.

Chokehold: The use of a lateral vascular neck restraint, carotid restraint or other action that involves the placement of any part of a law enforcement officer's body on, or around, an individual's neck in a manner that limits the individual's breathing or blood flow with the intent of, or the result of, causing bodily injury, unconsciousness, or death.

Commission: The Massachusetts Peace Officer Standards and Training (POST) Commission as established in M.G.L. c.6E § 2.

Compliant Individual: An individual who is fully cooperative with a Department member.

Deadly Force: UOF intended to inflict, or reasonably be expected to cause, death or serious physical injury.

- Members may not use deadly force against an individual who poses only a danger to themselves.
- Deadly force shall not be used at any point in time when there is no longer an objectively reasonable belief than an individual currently and actively poses an immediate threat of serious bodily harm or death, even if deadly force would have been justified at an earlier point in time.

De-escalation Tactics: Proactive approaches to stabilize a law enforcement situation so that more time, options, and resources are available to gain voluntary compliance and reduce or eliminate the need for force. These approaches may include, but not be limited to:

- Verbal persuasion;
- Warnings;

Definitions, continued

- Slowing down the pace of an incident;
- Waiting out an individual;
- Creating distance between the member and a threat;
- Requesting additional resources, including, but not limited to, licensed medical or mental health professionals, as defined in M.G.L. c. 111 § 51 ½ (a), when appropriate, to address a potential medical or mental health crisis; and
- Issuing a summons as an alternative to arrest where feasible.

Force: The amount of physical effort, however slight, required by police to compel compliance by an unwilling individual.

- Physically escorting or handcuffing an individual with minimal or no resistance does not constitute a UOF for the purposes of 550 CMR 6.03.
- UOF ***does include*** the pointing of a firearm or Electronic Control Weapon at an individual, and the use of OC spray on an individual or directed towards an individual.

Less-Lethal Force: Any physical UOF, other than deadly force, to control, restrain, or overcome the resistance of another.

- Members are authorized to use less-lethal force in accordance with all applicable federal and state laws and regulations and the contents of this policy.

Objectively Reasonable: This term means that, in determining the necessity for and appropriate level of force, officers shall evaluate each situation in light of the known circumstances, including, but not limited to, the seriousness of the crime, the level of threat or resistance presented by the subject, and the danger to the officer, subject, or community. The reasonableness of a particular use of force must be judged from the perspective of a reasonable officer on scene, rather than with the 20/20 vision of hindsight. Determining reasonableness of force must allow for the fact that police officers are often required to make instantaneous judgments in circumstances that are tense, uncertain and rapidly evolving. The force used must be reasonable under the circumstances known to the officer at the time force is used. *Graham v. Connor* 490 U.S. 386 (1989)

Officer-Involved Injury or Death: Any event during which an officer:

- Discharges a firearm, actually or proximately causing injury or death to another;
- Discharges any stun gun. actually or proximately causing injury or death to another;
- Uses a chokehold, actually or proximately causing injury or death of another;
- Discharges tear gas or other chemical weapon, actually or proximately causing injury or death of another;
- Discharges rubber pellets from a propulsion device, actually or proximately causing injury or death of another;

Definitions, continued

- Deploys a dog, actually or proximately causing injury or death of another;
- Uses deadly force, actually or proximately causing injury or death of another;
  Fails to intervene, to prevent the use of excessive or prohibited force by another officer who actually or proximately causes injury or death of another; or
- Engages in a physical altercation with a person who sustains serious bodily injury, or requests, or receives medical care as a result.

Passively Resistant Individual: An individual who is non-violent and uncooperative but does not use physical strength or body movement to resist a Department member and does not pose an immediate threat to the member or the public.

- A law enforcement officer shall only use the amount of force necessary against an individual who is engaged in passive resistance to effect the lawful arrest or detention of said individual and shall use de-escalation tactics where feasible, including issuing a summons instead of executing an arrest where feasible.

Proper Medical Aid: Immediate first aid treatment, including CPR, administered on the scene of an incident/injury within the scope of the member's training. Additionally, medical aid includes the summoning of emergency medical services to assist in any condition or treatment that may escalate outside of the scope of the capabilities of the member(s) providing immediate first aid or requiring transportation to a medical facility based on the condition of the person receiving aid.

Reportable Incident: Shall include:

- Pointing of a firearm or Electronic Controlled Weapon (ECW) at an individual;
- Application of force through the use of deadly or less-lethal weapons;
- On-duty discharge of any weapon outside of a training range specifically designed for that purpose;
- Off-duty discharge of a Department weapon outside of a training range specifically designed for that purpose;
- Department issued ECW activation, drive stun and/or probe, on or off duty, as defined in UOF-06 Electronic Control Weapons;
- Compliance or striking techniques are used;
- Use of OC spray on an individual or directed toward an individual; or
- UOF which actually, or proximately, caused or is reported to have caused injury or death to another.

Sensitive Population Groups: Sensitive population groups include those who reasonably appear to be, or are known to be, children, elderly, medically infirm, pregnant, or users of a cardiac pacemaker.

Serious Bodily Injury: Injury that results in or involves a substantial risk of death, permanent or protracted disfigurement, or extended loss or impairment of the function of a body part or organ.

De-Escalation Mandates

A member shall not use *force* upon another individual unless:

- De-escalation tactics have been attempted and failed or such tactics are not feasible based on the totality of the circumstances and such force is necessary and proportionate to:
    - Effect the lawful arrest or detention of an individual;
    - Prevent the escape from custody of an individual;
    - Prevent imminent harm and the amount of force used is proportionate to the threat of imminent harm, while protecting the safety of the member(s) or others; or
    - Defend against an individual who initiates force against a member;
    - Provided, however, that a law enforcement officer may use necessary, proportionate and non-deadly force in accordance with the regulations promulgated jointly by the POST commission and the Municipal Police Training Committee.

A member shall not use *deadly force* unless:

- De-escalation tactics have been attempted and failed, or such tactics are not feasible based on the totality of the circumstances; and
- Such force is necessary to prevent imminent harm to an individual, and the amount of force used is proportionate to the threat of imminent harm, and;
    - The imminent harm poses an imminent danger of death or serious bodily injury to the member or another individual;
    - The member attempts as many de-escalation tactics as feasible under the circumstances, including utilizing barriers where feasible; and
    - The member uses only the amount of force that is objectively reasonable.

Subject	Number
Use of Force	**UOF-01**

Duty to Intervene & Report

If a member observes another officer using, or attempting to use, physical force, including deadly force, beyond that which is necessary or objectively reasonable based on the totality of the circumstances, they shall intervene to prevent the use of unnecessary or unreasonable force, regardless of the rank of the officer so observed, unless intervening would result in imminent harm to the member or another individual.

Failure to intervene may subject a member to disciplinary action, civil liability, and/or criminal prosecution.

Per MGL c. 6E §10 (a) (xv): The Commission shall, after a hearing, revoke an officer's certification if the Commission finds by clear and convincing evidence that the officer failed to intervene, or attempt to intervene, to prevent another officer from engaging in prohibited conduct or behavior, including, but not limited to, excessive or prohibited force in violation of MGL c.6E §15.

Per MGL c.6E §10 (d)(viii): The Commission may, after a hearing, order retraining for any officer if the Commission finds substantial evidence that a law enforcement officer: fails to intervene to prevent another law enforcement officer from engaging in prohibited conduct or behavior, except a failure to intervene in conduct that mandates revocation pursuant to said subsection (a).

Reports of abuse by law enforcement personnel including, but not limited to, law enforcement officers, shall be made without fear of retaliation, or actual retaliation.

Any harassment, intimidation or retaliation against any law enforcement officer who either intervened to prevent or stop an excessive force incident, or made, intended to make, or is required to make a report regarding the witnessed excessive force incident shall be reported immediately to an appropriate supervisor and will not be tolerated. Any such actions may result in de-certification by the Commission.

Retaliation is prohibited against any employee who observes and reports an instance of using physical force, including deadly force, beyond that which is necessary or objectively reasonable based on the totality of the circumstances. This includes the discharge of the employee, any change to their official rank, grade or compensation, denial of a promotion or taking any other adverse action against said employee, or threatening to take any such action for providing information to the Department or testifying in any Department hearing or at any court proceeding resulting, or for providing information to the POST or testifying in any POST proceeding resulting.

Duty to Intervene Reporting Requirements

Position	Requirements
Observing Member	• Report the incident to an immediate on-duty Supervisor, not involved in the incident, as soon as reasonably possible, but no later than the end of the member's shift. This reporting shall documented in the daily administrative journal to include the name of the Supervisor the initial report was made; and • Within 24 hours of the initial report, absent extenuating-documented circumstances, submit to the Supervisor whom the initial report was made, a detailed written report describing the incident consistent with uniform reporting protocols.
Supervisor	• Notify the Troop Duty Officer of jurisdiction of the report; • Conduct and document a preliminary investigation to gather the pertinent facts and information required for a follow-on investigation; • Prepare a detailed written report documenting the member's report, steps taken by the Supervisor upon receipt of the member's report, and subsequent investigative actions; and o The reporting member's written report shall be included in the Supervisor's report. o If the reporting member is unable to provide a written report, due to extenuating-documented circumstances, the Supervisor shall utilize the initial report as the foundation for their subsequent written report. • Submit their written report to their Troop/Section Commander within 24 hours.
Troop Duty Officer	• Assign a Supervisor to conduct an investigation, if the observing member reports the incident to the Troop Duty Officer directly; • Document the initial report in the Troop HQ Daily Administrative Journal; and • Notify the Troop/Section Commander of the initial report upon receipt.
Troop/Section Commander	• Notify their Division Commander and the Division Commander of DST upon receipt of the initial report notification.
Division Commander-DST	• Initiate an investigation in accordance with Department guidelines.

Use of Force Responses

(Note: *UOF responses need not be exercised in progression*.)

Determining the level of force necessary may depend on resistance levels and circumstances. Factors in this decision include, but are not limited to:

- Subject vs. member - relative to age, size, physical condition, skill level;
- Subject's drug and alcohol use;
- Weapons - type, proximity;
- Seriousness of offense;
- Exigent circumstances; and
- Number of potential assailants vs. number of law enforcement officers on the scene.

If the subject is…	Then the response may include…
Compliant	• Verbal commands
Passively Resistant	• Verbal commands; and/or • Contact control techniques.
Actively Resistant	• Verbal commands; • Contact control techniques; • Compliance techniques; • Distraction techniques; • Oleoresin Capsicum (OC) Spray, according to training; • Laser activation of Electronic Control Weapon (ECW) according to training; • Warning Arc of Electronic Control Weapon (ECW) according to training; and • Drive Stun deployment of Electronic Control Weapon (ECW) according to training.
Assaultive-Bodily Harm	• All of the above responses; • Striking techniques; • Probe deployment of Electronic Control Weapon (ECW) according to training; and • Any other Department approved less-lethal force equipment.
Aggravated Assaultive - Serious Bodily Harm /Death	• All of the above responses; and • Deadly force.

Use of Force

Verbal Commands
Commands and gestures designed to:
- Effect compliance; and
- Express the member's intent.

Contact Control Techniques
Touch techniques (carrying and guiding) not designed to produce pain compliance.

Compliance Techniques
Techniques authorized by the Department that may be used to achieve compliance and/or control of an actively resistant or assaultive subject.

In exigent circumstances, other compliance techniques may be used.

Distraction Techniques
Techniques intended to temporarily break the mental focus of an actively resisting individual and create an opportunity for the member to apply a compliance or control technique. Distraction techniques may be similar to striking techniques, but they differ in *intent* and *intensity*. The *intent* is to take the subject's focus off of their chosen method of resistance so that the member can bring them under control, unlike a striking technique, where the intent is to stop an assault. The *intensity* is, therefore, less than it would be with a striking technique. The intensity of the distraction technique should be limited so as not to create substantial trauma or lasting injury.

OC Spray
OC spray may be used in situations involving:
- Assaultive subjects; or
- Actively Resistant subjects when:
  - Verbal commands have failed to bring about compliance; and
  - Subject has signaled their intentions to actively resist.

OC spray shall not be used on passive resisters who offer **NO** physical resistance.

Striking Techniques
Striking techniques may be used on an assaultive subject to achieve compliance and/or control.

Striking techniques may include the use of issued equipment (e.g., baton, flashlight), as well as hands, feet, elbows, or knees.

In exigent circumstances, other instrumentalities may be used.

Electronic Control Weapons (ECW)
Department Members are authorized to use ECW in accordance with Department training and UOF-06 *Electronic Control Weapons.*

Subject	Number
Use of Force	**UOF-01**

Use of Deadly Force: Preventing Escape	Members are authorized to use deadly force to prevent the escape of a suspect when the member has probable cause to believe that:
	• The arrest is for a felony; and
	• The member believes that the force employed creates no substantial risk of injury to innocent persons; and either:
	  ○ The crime for which the arrest is made involved conduct including the use or threatened use of deadly force; or
	  ○ There is a substantial risk that the individual to be arrested will cause death or serious bodily harm / serious physical injuries if the suspect's apprehension is delayed; and
	• If feasible, some clear, verbal warning has been given.

A member <u>may</u> discharge a firearm for:	• The lawful performance of duties; • On or off duty training at a range, specifically designed for that purpose and using only Department authorized ammunition; or • Rendering harmless an animal that represents a threat to public safety or is seriously injured and suffering.
A member **<u>SHALL NOT</u>** discharge a firearm:	• As a warning.

Subject	Number
Use of Force	**UOF-01**

Discharge of a Firearm At a Moving Motor Vehicle	**Members shall:** • As a first course of action, remove themselves from the path of a moving vehicle or position of vulnerability; and • Understand and consider that: o Bullets fired at moving vehicles are unlikely to stop or disable the motor vehicle; o Bullets fired may miss the intended target or ricochet and cause injury to themselves, other officers, or innocent persons; or o If the bullets disable the operator, the vehicle may crash and cause injury to themselves, other officers, or innocent persons. **A member SHALL NOT discharge a firearm:** • To merely disable a fleeing vehicle; or • At, into, or from a moving vehicle, **UNLESS,** based on the totality of the circumstances, including the risk of safety to other persons in the area, such discharge is objectively reasonable, necessary to prevent imminent harm to a person and the discharge is proportionate to the threat of imminent harm and only if the following conditions exist: o An individual in the vehicle is threatening the member or another person with deadly force by means other than the vehicle; or the vehicle is operated in a manner deliberately intended to strike a member or another person, and all other reasonable means of defense have been exhausted or are not present or practical, which includes moving out of the path of the vehicle; o Member(s) have not intentionally positioned themselves in such a way as to create a likelihood of being struck by an occupied vehicle (e.g., surrounding a vehicle at close proximity while dismounted); o The member is not discharging the firearm strictly to disable the vehicle; and The circumstances provide a high probability of stopping or striking the intended target.

Ready Position	When the member reasonably believes that there is a potential threat of serious bodily harm/serious physical injuries or death, the firearm may be placed at the ready position: • Trigger finger is alongside of the frame except when ready to engage; and • In a safe direction, below the line of sight, so as not to impede member's vision.

Subject	Number
Use of Force	**UOF-01**

Use of Force Equipment and Training	The Colonel/Superintendent shall authorize the specific UOF equipment and training to be used by members. Members are responsible for keeping their equipment clean and operational at all times. All members shall successfully complete training and be certified in the specific UOF equipment prior to being authorized to carry or use such force options and/or equipment.

Investigations/ Reporting

The reporting and investigation of UOF by a member shall be in accordance with UOF-03 Use of Force Reporting, initiated upon any UOF reportable incident.

Temporary Relief from Duty

A member, whose action(s) or UOF in an official capacity results in death or serious bodily injury shall:

- Be placed on administrative leave in accordance with Article 6. A duty status board shall be convened to review the actions of the member and recommend the appropriate duty status.

References

UOF-03 Use of Force Reports;
UOF-06 Electronic Controlled Weapons (ECW);
M.G.L. c.6E: § 10 (a), §14 (a) through (d), § 15 (a) and (b);
550 CMR 6.00 *et seq.*;
MPAC: 1.1.1, 1.1.2, 1.1.3, 1.1.5, 1.1.8, 26.0.4;
Presidential Executive Order No. 13929;
United States Department of Justice: Standards for Certification on Safe Policing for Safe Communities. (E.O. No. 13929);
TASER 7 CEW User Course (Version 22);
TASER Energy Weapon Master Instructor One Day Instructor Course Drill Booklet.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**UOF-02**
Subject:	
Use of Force Response	

Policy

The Department shall immediately respond to the scene and conduct an investigation when a use of force results in:

- A death;
- Serious bodily injury; and/or
- Any reportable discharge of a firearm per UOF-03 Reports.

Firearm discharge not requiring an investigation:

- Authorized testing in a properly controlled environment (e.g. Armorer, Ballistician); or
- A firearm is discharged at a range, specifically designed for training and using only Department authorized ammunition; or
- Rendering harmless an animal that is seriously injured and suffering.

For the purpose of this policy, the term "member" shall apply to sworn members of the Department; the term "employee" shall apply to civilian non-sworn members of the Department.

Definitions

Deadly Force: Use of force intended to inflict, or reasonably be expected to cause, death or serious physical injury.

Less-Lethal Force: Any physical use of force, other than deadly force, to control, restrain, or overcome the resistance of another. 550 CMR 6.03

Serious Bodily Injury: Injury that results in or involves a substantial risk of death, permanent or protracted disfigurement, or extended loss or impairment of the function of a body part or organ.

Officer-Involved Use of Deadly Force Investigation

Fatal

When a Department member is involved in a use of deadly force resulting in a fatality, the District Attorney's Office or State Police Detective Unit (SPDU) of jurisdiction shall direct the investigation.

Non-Fatal

When a Department member is involved in a use of deadly force **not** resulting in a fatality, the Division of Investigative Services (DIS) Major who oversees the area where the incident occurs shall assign a Commissioned Officer from DIS to conduct an investigation.

Force Investigation Response and Support Team (FIRST)

The Force Investigation Response and Support Team (FIRST) shall:

- Be comprised of Commissioned Officers designated by the Colonel/Superintendent;
- Be assigned to regional teams; and
- Assist the DIS Commander.

FIRST Activation

Upon notification of an incident resulting in the use of deadly force, the Communications Section shall notify:

- The DIS Commander or designee; and
- The SPDU Commander of jurisdiction.

The DIS Commander or designee shall dispatch the FIRST.

FIRST Duties

The DIS Commander or designee shall determine the duties of the FIRST which may include:

- Verify that the following has occurred:
  - The scene is safe and secure;
  - A perimeter has been established;
  - Threats have been eliminated; and
  - Any suspect(s) have been secured.
- Verify that all proper notifications are made, through channels to the Colonel/Superintendent;
- Identify a controlled area for on-scene interviews and conduct interviews where appropriate;
- Verify that individuals are advised of their rights; and
- Coordinate with the assigned DIS investigator to notify next of kin of all law enforcement and/or civilian victims in accordance with ADM-12 Serious Injury/Death of a Member, if necessary.

Weapons Seizure

The first responding Supervisor shall:

- Immediately seize or take custody of involved weapons and magazines (if applicable);
- Transfer custody of the seized weapon to the Firearms Identification Section (FIS); and
- Assist the FIS and Crime Scene Services personnel in the processing of evidence.

Crime Scene Services

Crime Scene Services shall:

- Respond to the scene and coordinate all Crime Scene Services activities with the assigned DIS investigator;
- Gather all evidence at the scene in accordance with INV-10 Evidence Collection/Preservation; and
- Map, photograph, and videotape the scene, if necessary.

Interviews

Interviews with involved Department members shall be:

- Conducted by a Commissioned Officer, as directed by the assigned DIS investigator.

Interviews with civilian witnesses may be:

- Conducted by Commissioned and/or Non-Commissioned Officers as directed by the assigned DIS investigator.

Troop/Section Commanders

The Troop/Section Commanders of jurisdiction shall:

- Establish intra-agency cooperation in conjunction with the assigned DIS investigator.

Firearms Identification Section

If a firearm is involved, a member of the FIS shall:

- Respond to the scene, take custody of any involved firearms, and begin a firearms related investigation; and
- Notify the Armorer when a Department firearm is removed from service.

If appropriate, a temporary firearm shall be issued by the Armorer or designee, as specified in ADM-20 Weapons Management.

Members Using Force

A member involved in a use of force incident resulting in death or serious bodily injury shall:

- Surrender use of force equipment **only** to a Department Supervisor;
- Absent an injury, incapacitation, or other exigent circumstances:
  - Submit a detailed written report not less than twenty-four (24) hours, nor more than forty-eight (48) hours after the incident; or
  - Submit to an interview by a Commissioned Officer involved in the investigation, in lieu of a written report, subject to all rights under applicable laws and collective bargaining agreements; and
  - Submit a SP 376 Use of Force Report to the assigned DIS Investigator, within twenty-four (24) hours of the incident.
- Submit to a follow-up interview, if necessary; and
- Be allowed to contact a union representative, if desired.

Temporary Relief from Duty

Sworn Department Members:
A sworn member whose action(s) or use of force in an official capacity results in death or serious physical injury shall:

Be placed on administrative leave with pay in accordance with Article 6. A duty status board shall be convened to review the actions of the member, and recommend the appropriate duty status.

When involved in a shooting a sworn member shall be placed on Administrative Leave with pay for up to five (5) work days.

Civilian Department Employees:
Civilian employees of the Department whose actions, in an official capacity, have resulted in death and/or serious physical injury of another party may be removed from their assignment and placed on administrative leave with pay pending an administrative review and/or investigation conducted in accordance with the Commonwealth Human Resources Division's regulations and policies and any applicable collective bargaining agreement.

Medical Evaluations

A member shall undergo a medical evaluation by the State Police Surgeon prior to returning to duty from any period of Administrative Leave following a shooting, or when a member's actions result in a death.

Employee Assistance Unit

Members and employees are strongly encouraged to contact the Employee Assistance Unit (EAU) for additional support and assistance.

Follow-up counseling and assistance shall be provided by the EAU as needed.

The EAU shall also assist members and employees in obtaining support resources outside the Department.

Responsibilities and Protocol

Position	Responsibilities
All Members at Scene	• Administer and secure medical aid after any use of force, if necessary; • Protect and secure the scene; • Ensure the Desk Officer has been notified; • Speak only to Department investigators, unless otherwise ordered by a member of the Command Staff; and • May consult an attorney.
Desk Officer	• Dispatch necessary assistance to the scene; • Notify Troop Duty Officer and Station Commander; • Make appropriate Records Management System entries; and • Refer media inquiries to the Media Relations Section or the District Attorney's Office.
Troop Duty Officer	• Dispatch to the scene a Supervisor who is at least one rank higher than the involved member; • Notify Troop Commander; • Notify appropriate DIS on-call representative; • Notify GHQ Communications Duty Officer; • Make appropriate Records Management System entries; and • Refer media inquiries to the Media Relations Section or the District Attorney's Office.
Supervisors	• Ensure EMS has been notified and determine the condition of all members and civilians at the scene; • Ensure involved weapon(s) have been seized and secured; • Ensure the area has been secured and limit entry to the scene; • Record and document all members present at the scene in the on-scene access control log; • Keep Troop Duty Officer informed; and • Refer media inquiries to the Media Relations Section or the District Attorney's Office.

Responsibilities and Protocol, continued

Position	Responsibilities
GHQ Communications	• Notify Colonel/Superintendent; • Notify DIS Commander or designee; • Ensure appropriate DIS on-call representative has been notified; • Notify Media Relations Section; and • Notify Employee Assistance Unit.
Lead DIS Investigator	• Assume control of the scene; • Coordinate actions with the Troop Commander and/or DIS Commander or designee; • Before interviewing or requesting written statements, advise the involved member(s) of their rights, if the member is suspected of violating the law; and • Review and submit a SP 376.
Troop Commander of Jurisdiction	• Notify Division Commander of involved member(s); • Proceed directly to scene in incidents of death or serious bodily injury; and • Assist the media pending arrival of the Media Relations Section.
Division Commander of Member(s) Involved	• Appoint a Commissioned Officer to conduct an Administrative Review of the final report issued by the assigned DIS Supervisor responsible for the investigation. • Note: The Administrative Review is to ensure that members followed Department procedures during the incident.
Colonel/ Superintendent	• Notify Executive Office of Public Safety and Security (EOPSS).

References: ADM-12 Serious Injury/Death of a Member;
ADM-20 Weapons Management;
INV-10 Evidence Collection/Preservation;
SUP-04 Employee Assistance Unit;
SP 376 Use of Force Report;
550 CMR 6.09;
MPAC: 1.1.6, 1.1.7, 1.1.8.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

2211

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**UOF-03**
Subject:	
Use of Force Reporting	

Policy

All incidents involving the use of force (UOF) shall be documented.

Members shall adhere to the Duty to Intervene and Report mandates of General Order UOF-01, Use of Force.

The Department shall report to the National Use of Force Data Collection Database when actions by a member resulted in the death or serious bodily injury of an individual, or when a member, in the absence of death or serious bodily injury, discharged a firearm at, or in the direction of an individual.

Definition

Commission: The Massachusetts Peace Officer Standards and Training (POST) Commission as established in M.G.L. c.6E § 2.

Deadly Force: Use of force intended to inflict, or reasonably be expected to cause, death or serious physical injury.

Force: The amount of physical effort, however slight, required by police to compel compliance by an unwilling individual.

- Physically escorting or handcuffing an individual with minimal or no resistance does not constitute a use of force for the purposes of 550 CMR 6.03.
- Use of force ***does include*** the pointing of a firearm or Electronic Control Weapon at an individual, and the use of OC spray on an individual or directed towards an individual.

Less-Lethal Force: Any physical use of force, other than deadly force, to control, restrain, or overcome the resistance of another.

Reportable Incident: Shall include:

- Pointing of a firearm or Electronic Control Weapon (ECW) at an individual;
- Application of force through the use of deadly or less-lethal weapons;
- On-duty discharge of any weapon outside of a training range specifically designed for that purpose;
- Off-duty discharge of a Department weapon outside of a training range specifically designed for that purpose;
- Department issued ECW activation, drive stun and/or probe, on or off duty, as defined in UOF-06 Electronic Control Weapons;
- Compliance or striking techniques are used;

Definition, continued

- Use of OC spray on an individual or directed toward an individual; or
- Use of force which actually, or proximately, caused or is reported to have caused injury or death to another.

Serious Bodily Injury: Injury that results in or involves a substantial risk of death, permanent or protracted disfigurement, or extended loss or impairment of the function of a body part or organ.

Use of Force Reporting

Any reportable incident, as defined above, shall be reported to the Station Desk Officer of jurisdiction and documented within the Records Management System.

The involved member(s) shall:

- Submit a SP 376 *Use of Force Report* along with the SP12 or To/From within twenty-four (24) hours of the incident, absent an injury, incapacitation, or other circumstances, with approval from their Division Commander; and
- TASER X2: Ensure that Station/Unit Commander or Designee is provided access to ECW for downloading purposes.
- TASER 7: Place the battery in a dock within 24 hours of a reportable incident and ensure data upload is completed.

A member who knowingly makes an untruthful statement concerning a material fact or knowingly omits a material fact from a use of force report may be subject to de-certification by the Commission.

Use of Force Review

Supervisory/Administrative reviews of UOF incidents shall not be conducted by a member involved in the use of force incident under review.

Supervisors shall:

- Ensure members submit a SP 376 along with the SP12 or To/From;
- Review every SP 376 and SP12 or To/From; and
- Forward all reports to the Division Commander, through channels with findings and recommendations as to the necessity of further investigation of the incident no later than 5 business days from receipt of the SP 376.

Station/Unit Commander or Designee Shall:

- Ensure that ECW data is downloaded per manufacturer instructions; and
- Ensure that data from ECW download is consistent with reports submitted by involved member(s).

The Troop Commander and/or Detective Captain of jurisdiction:

- Shall assign a Commissioned Officer to conduct an administrative review of the use of deadly force; or
- May assign a Commissioned Officer to conduct an administrative investigation of the use of less-lethal force.

Use of Force Review, continued

Division Commanders shall:

- Forward a copy of all reports, through channels, to the Division of Standards and Training; and
- Forward a copy of all reports to the Use of Force Review Committee.

Division of Standards and Training Commander may:

- Provide a copy of each report involving the discharge of a firearm to the Director of Firearms Training.

Use of Force Review Committee

The Deputy Superintendent shall appoint members of the UOF Review Committee. The UOF Review Committee shall evaluate each use of force incident and forward their findings and recommendations to the Deputy Superintendent.

Use of Force Review Committee Evaluation

The Committee shall determine that the UOF was:

- Within Department guidelines; or
- Outside Department guidelines.

The Committee's evaluations and recommendations shall include:

- Tactics and training considerations;
- Supervision considerations;
- Department directives; and
- The need for further Department action.

Classifications of weapons discharge include:

- Intentional: deliberate discharge;
- Unintentional: when a member does in fact depress the trigger and causes the firearm to discharge without consciously or deliberately wanting to do so; or
- Accidental: restricted to the description of a mechanical flaw, shortcoming, or breakdown of a firearm that occurs from such causes as excessive wear, corrosion, mechanical design, or a part breakage, which would allow the weapon to discharge without the shooter depressing the trigger; and
- Other findings as necessary.

Use of Force Reports Records

The Committee shall maintain in the Deputy Superintendent's Office, a secure file of all UOF Reports, investigations, and reviews.

The Committee shall prepare an annual report analyzing Department UOF reporting. The report shall summarize annual UOF statistics, the findings on any patterns or trends identified and a finding on whether any changes are needed in agency policies, practices, equipment, or training. The annual report shall be provided to the Colonel/Superintendent.

Subject:	Number:
Use of Force Reporting	**UOF-03**

References: UOF-01 Use of Force;
UOF-06 Electronic Control Weapons;
SP 376 Use of Force Report;
550 CMR 6.00 *et seq.*;
MPAC: 1.1.6, 1.1.7, 1.1.14, 82.2.4.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

2315

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**UOF-04**
Subject:	
Use of Force-Equipment	

Policy

Members on-duty shall carry and use only Department issued use of force (UOF) equipment for which they have received Department approved training and maintain a current certification.

Definition

Gun Safe: a safe, gun safe, gun case, lock box, or other device that is designed to be or can be used to store a firearm and that is designed to be unlocked only by means of a key, a combination, or other similar means in accordance with M.G.L. C. 140 §131.

Use of Force Equipment: All equipment approved by the Colonel/ Superintendent and issued by the Department including, but not limited to, firearms, ammunition, Oleoresin Capsicum (OC) Spray, batons, Electronic Control Weapons (ECW), and/or any other equipment used to effect control and compliance of a subject.

Purchase/ Issuance

Title	Duties
Colonel/ Superintendent	• Shall approve all UOF equipment issued and utilized by the Department; and • Shall authorize, in writing, the Division of Administrative Services (DAS) to purchase all UOF equipment issued and utilized by the Department.
Division of Administrative Services (DAS)	• Is solely responsible and solely authorized to purchase any and all UOF equipment issued and utilized by the Department; and • Shall purchase any and all UOF equipment issued and utilized by the Department pursuant to the written authorization of the Colonel/Superintendent or designee.

Purchase/ Issuance, continued

Title	Duties
Armorer	• Shall test and recommend UOF equipment, including ammunition, through channels to the Office of the Superintendent or designee; • Issue and maintain UOF equipment; • Document and retain all records related to UOF equipment; • Maintain and update the UOF Master Equipment List approved by the Colonel/Superintendent; • Inspect and approve all weapons authorized to be used in the performance of duty before issuance; • Inspect and re-issue UOF equipment, turned in by members, that is operational and in good working order; and • Replace UOF equipment as needed.

Inspections

All UOF equipment shall be inspected for condition and operational readiness, only by a supervisor trained to inspect such equipment. Inspection(s) shall be documented in the appropriate Department database.

Supervisors shall:
- Remove from service any UOF equipment found to be defective; and
- Notify the Armorer when a Department firearm or ECW is removed from service.

Title	Duty	Occurrence
Commanders/ Supervisors	Direct/conduct an inspection of all UOF equipment of those under their supervision.	Quarterly
UOF Instructors/ Armorer	Conduct and document an inspection of all UOF equipment as applicable.	Initial issuance and/or requalification.
Office of Professional Integrity & Accountability	Conduct an inspection of all UOF equipment.	As appropriate

Maintenance

All UOF equipment shall be kept clean and operational at all times.

Issued firearms shall be cleaned promptly after training:
- In a safe location and manner; and
- Prior to leaving any range.

Only the Armorer and personnel authorized by the Armorer shall repair or modify any UOF equipment or parts.

ON DUTY Carry/Security

While on duty:

- Uniformed members shall carry issued sidearms secured in an issued holster; and
- Non-uniformed members shall carry issued sidearms secured in an issued holster, or otherwise authorized holster, as approved by the Colonel/Superintendent.

When carrying issued firearms, members shall do so in a safe and secure manner:

- Sidearms shall be fully loaded with a round in the chamber and the weapon de-cocked, if equipped;
- Desk Officers shall carry their sidearm in their holster on their person;
- Firearms shall not be left unattended in any non-secure location such as a desk drawer or file cabinet; and
- Firearms and ECWs **shall not** be carried on a member's person during the booking process, including (but not limited to) booking, fingerprinting, and the administration of the breath test.

OFF DUTY Carry/Security

Only Department issued/trained/approved firearms, ammunition and UOF equipment are authorized for members performing official police duties and responsibilities off-duty.

Members are not required to carry any Department issued firearm, ammunition or UOF equipment while off-duty.

Members carrying a firearm, ammunition or UOF equipment not issued/trained/approved by the Department shall comply with the licensing restrictions set forth in M.G.L. C. 140 §131 and MSP Policy, Rules & Regulations.

Indemnification of off-duty use of force actions shall be determined in accordance with M.G.L. C. 258 §9A.

When carrying a Department issued firearm off duty, the following items shall be in the member's possession:

- The member's Department's Badge of Office;
- The member's Department's Identification Card; and
- The member's active License to Carry a Firearm.

When issued firearms are not being carried, they shall be secured with the issued firearm lock and/or in a gun safe, inaccessible to children and others.

OFF DUTY Carry/Security, continued

Members are not authorized to carry their Department issued ECW while off-duty.

When off-duty, members shall secure Department issued ECWs in a manner consistent with the securing of a firearm and in accordance with all applicable Massachusetts Laws. Members must ensure that Department issued ECWs are inaccessible to children and others.

Firearms in Vehicles

Firearms shall not be left unattended in any vehicle, unless the vehicle is a Department issued vehicle for which the Department has authorized a gun safe or other device designed to secure the weapon and the firearm is secured in such a device. When a member stores a firearm in such a device within an unattended Department vehicle, the device shall be locked and secured, the vehicle's windows shall be closed, and the vehicle's doors shall be closed and locked.

Examples of properly secured weapons:

Patrol Rifle:

- The patrol rifle shall be secured in the Department installed gun rack in accordance with the patrol rifle standard operating procedures.

Shotgun:

- The shotgun shall be secured in the Department installed gun rack, in accordance with shotgun standard operating procedures; and
- If equipped, the key lock shall be engaged when the vehicle is unattended.

STOP Team:

- Firearms shall be secured in accordance with STOP Team standard operating procedures.

Vehicle Safe Requests:

Members requesting to install a gun safe within Department vehicles shall:

- Submit a written request for approval to their Division Commander articulating the need for such a device;
- If approved, coordinate with the Fleet Administrator regarding the professional installation of the safe and regarding the location of installation within the vehicle; and
- Agree, in writing, to assume all responsibility for:
  - The loss or theft of the safe; and
  - Any damage caused to the vehicle associated with the installation or removal of the safe.

, continued

The Armorer shall:

- Determine and approve the make and model of all gun safes to be issued by the Department; and
- Advise the Fleet Administrator of the gun safes authorized for purchase.

Division Commanders shall forward all gun safe requests, whether approved or denied, to the Fleet Administrator.

Soft Body Armor

Soft body armor shall be issued to members with the intent that it be worn as often as possible, while on duty.

Members who decline to wear the issued soft body armor shall submit a letter to the appropriate Division Commander stating their reasons. Issued soft body armor a member declines to wear shall be stored and readily accessible in the member's cruiser.

References: M.G.L. C.140 §131;
M.G.L. C.258 §9A;
MPAC: 1.1.9, 1.1.10, 41.3.5.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**UOF-05**

Subject:

Use of Force Training

Policy

The Department shall provide training and instruction to every member to become proficient in the use of issued weapons and control techniques.

Training and proficiency testing shall be provided by instructors certified in the weapon(s) and/or technique(s) they are providing instruction/testing on.

All members shall successfully complete approved training, qualify and be certified with weapons and techniques prior to use.

The Department shall provide pre-service training to trainees and annual training to sworn members on de-escalation tactics.

Training protocols shall adhere to, or exceed, applicable federal and state laws and regulations for members to become, and remain in, good standing as law enforcement officers. The Department's training protocols shall include substantive instruction on the agency's use of force (UOF) policies and procedures, de-escalation techniques, and related legal updates.

Members ***shall not use*** a chokehold or other tactics that restrict or obstruct an individual's breathing or oxygen or blood flow to an individual's head or neck. Members shall not be trained to use a lateral vascular neck restraint, carotid restraint or other action that involves the placement of any part of the Member's body on or around an individual's neck in a manner that limits the individual's breathing or blood flow.

Except to temporarily gain, regain or maintain control of an individual and apply restraints, a Member ***shall not*** intentionally sit, kneel, or stand on an individual's chest, neck, or spine, and shall not force an individual to lie on their stomach.

A Member ***shall not*** obstruct the airway or limit the breathing of any individual, nor shall a Member restrict oxygen or blood flow to an individual's head or neck. An individual placed on their stomach during restraint should be moved into a recovery position or seated position as soon as possible.

Instructors shall document and provide to the Academy Director of Training all training records including, but not limited to, approved lesson plans, dissemination and instruction of applicable policies, attendance records, proficiency-test results and related training materials.

Definitions

Chokehold: The use of a lateral vascular neck restrain, carotid restraint or other action that involves the placement of any part of a law enforcement officer's body on, or around, a person's neck in a manner that limits the person's breathing or blood flow with the intent of, or the result of, causing bodily injury, unconsciousness or death.

Deadly Force: Use of force intended to inflict, or reasonably be expected to cause, death or serious physical injury.

- Members may not use deadly force against an individual who poses only a danger to themselves.
- Deadly force shall not be used at any point in time when there is no longer an objectively reasonable belief than an individual currently and actively poses an immediate threat of serious bodily harm or death, even if deadly force would have been justified at an earlier point in time.

De-escalation Tactics: Proactive approaches to stabilize a law enforcement situation so that more time, options, and resources are available to gain voluntary compliance and reduce or eliminate the need for force. These approaches may include, but not be limited to:

- Verbal persuasion;
- Warnings;
- Slowing down the pace of an incident;
- Waiting out an individual;
- Creating distance between the member and a threat;
- Requesting additional resources, including, but not limited to, licensed medical or mental health professionals, as defined in M.G.L. c. 111 § 51 ½ (a), when appropriate, to address a potential medical or mental health crisis; and
- Issuing a summons as an alternative to arrest where feasible.

Force: The amount of physical effort, however slight, required by police to compel compliance by an unwilling individual.

- Physically escorting or handcuffing an individual with minimal or no resistance does not constitute a use of force for the purposes of 550 CMR 6.03.
- Use of force ***does include*** the intentional pointing of a firearm or Electronic Control Weapon at an individual as an attempt to control that individual's movements, and the use of OC spray on an individual or directed towards an individual.

Less Lethal Force: Any physical use of force, other than deadly force, to control, restrain, or overcome the resistance of another.

Definitions, continued

- Members are authorized to use less lethal force in accordance with all applicable federal and state laws and regulations and the contents of this policy.

Specialized Firearms: Any firearm other than the primary duty pistol(s).

Training

Prior to being authorized to carry a lethal/less-lethal weapon, the instructor shall ensure members receive direction on access to, and instruction in the Department's UOF policies including, but not limited to:

- De-Escalation Tactics;
- Use of reasonable/necessary force;
- Use of deadly force;
- Warning shots (firearms training only);
- Authorized less-lethal weapons; and
- Rendering aid after the use of weapons and/or force.

The issuance and/or policy access direction, and instruction shall be documented in the UOF lesson plan.

At least annually, all Department members authorized to carry weapons shall receive in-service training on the Department's UOF policies, de-escalation tactics and demonstrate proficiency with all approved deadly weapons and electronic controlled weapons issued to the member. The administration of the training shall be documented and records maintained by the State Police Academy (SPA).

At least biennial (every 2 years) all Department members shall receive current in-service training and testing with less-lethal weapons including baton, Oleoresin Capsicum Spray (OC), any other less lethal weapons and weaponless control techniques. The administration of the training shall be documented and records maintained by the SPA.

- Members that are unable to qualify with less-lethal weapons or techniques will receive remedial training and demonstrate proficiency in same prior to resuming official duties.

Safety is of paramount importance. Regardless of a member's rank, certified UOF instructors shall be in command of all personnel and equipment during training.

Training shall, as closely as practicable, reflect the conditions with which members are likely to be confronted. This training shall include comprehensive instruction in:

- The Department's UOF directives and applicable standard operating procedures;
- Legal updates;
- Proficiency and safe weapons handling skills; and
- Safety, storage, and maintenance of UOF weapons and equipment.

Failure to Qualify with Firearms

Those members who fail to meet initial qualification and firearms handling standards shall receive immediate remedial assistance. Members may receive two (2) additional opportunities to qualify within the same day; unless the Supervisor of Firearms Training determines that it would be unsafe or impractical to do so.

In the event a member fails to achieve qualification standards after remedial assistance, the Division of Standards and Training Commander, or designee, shall immediately notify the Deputy Superintendent.

Firearms Remedial Training

Member(s) failing to initially qualify shall be assigned to the Range for the Remedial Training Program.

The Remedial Training Program shall consist of three phases designed to assist the remedial shooter in attaining firearms qualification standards. The content of the remedial program shall be determined by the Supervisor of Firearms Training.

- Phase 1 Remedial Training shall consist of one (1) training day;
- Phase 2 Remedial Training shall consist of two (2) training days; and
- Phase 3 Remedial Training shall consist of two (2) training days.

If a member fails to achieve firearms qualification standards after Phase 1 Remedial Training, the member shall be assigned to the Phase 2 Remedial Training.

If a member fails to achieve firearms qualification standards after the Phase 2 Remedial Training, the member shall be:

- Evaluated by the State Police Surgeon to determine if any physical limitation(s) exist that would prevent him/her from achieving the firearms qualification standards; and
- Assigned to the Phase 3 Remedial Training at the State Police Academy for more in-depth assistance.

When participating in any phase of the Remedial Training Program, it is mandatory that a member successfully complete two (2) consecutive runs of the qualification course.

If proficiency is not established at the end of the Remedial Training Program:

- The member shall immediately surrender all firearms and cruiser keys to the Supervisor of Firearms Training;
- The Supervisor of Firearms Training shall immediately secure the firearm(s) and cruiser and advise the Division of Standards and Training (DST) Commander or designee; and

Firearms Remedial Training, continued

- The DST Commander or designee, shall place the member on administrative leave with pay, and shall proceed with an administrative hearing in accordance with Articles 5 and 6 of the Rules and Regulations.

The Three Phase Remedial Training Program shall constitute reasonable efforts by the Department in an attempt to achieve qualification by a member.

Failure to qualify with issued firearms shall result in administrative action, up to and including termination of employment.

Specialized Firearms-Failure to Qualify

In the event that a member fails to achieve firearms qualification standards with Specialized Firearms after remedial training, the member shall:

- Be required to surrender such specialized firearms to the Supervisor of Firearms Training; and
- Be assigned to a one (1) day Specialized Firearms Remedial Training Program.

If proficiency is not established at the end of the Specialized Firearms Remedial Training Program, the member may:

- Receive additional remedial training at the discretion of the Colonel/Superintendent.

Qualification/ Other Use of Force Weapons

The DST Commander, or designee, shall establish standards for qualification with other UOF weapons prior to issuance.

Responsibilities

Position	Duties
Supervisor of UOF Training	• Conduct necessary training and testing; and • Maintain documentation on UOF training and proficiency, to include UOF policy training.
Division Commander of DST or designee	• Approve instructors; • Recommend training standards; and • Maintain program records.
Division Commanders	Ensure all members are trained as required.
Deputy Superintendent	Authorize all UOF training prior to implementation.
Colonel/Superintendent	Establish qualification standards.

Subject:	Number:
Use of Force Training	**UOF-05**

Extended Leaves of Absence

Members returning from a leave in excess of ninety (90) days shall comply with any and all training requirements in accordance with ADM-11E Extended Leaves of Absence.

References:

Articles 5 Rules of Conduct;
Article 6 Regulations Establishing Disciplinary Procedures and Temporary Relief from Duty;
ADM-11E Leaves of Absence;
M.G.L c. 6E § 14(c);
550 CMR 6.00 *et seq.*;
MPAC: 1.1.9, 1.1.10, 1.1.11, 1.1.12, 1.1.13.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

2326

Department of State Police
General Order

Effective Date:	Number:
May 25, 2023	**UOF-06**
Subject:	
Electronic Control Weapons (ECW)	

Policy

The Department shall provide proper, current guidance and direction on the use of Electronic Control Weapons (ECWs).

Only those Department members who have successfully completed the Department's initial ECW training and subsequent in-service ECW training are authorized to use an ECW.

Members are authorized to use only that force which is objectively reasonable, in accordance with all applicable federal and state laws and regulations, and the contents of this policy to:

- Effect the lawful arrest or detention of an individual;
- Prevent the escape from custody of an individual; or
- Prevent imminent harm, and the amount of force used is proportionate to the threat of imminent harm.

ECWs may be used by authorized, trained and certified Department members in accordance with all applicable federal and state laws and regulations, and the contents of this policy. Members shall use reasonable force to control individuals who are violent, exhibiting threatening or potentially violent behavior, or physically resisting arrest or detention.

Members should assess each situation to determine which action shall best bring the incident under control, using only that amount of force that is reasonably necessary.

If feasible, some clear, verbal warning shall be given before any use of force. Such warning should include identifying the member as a law enforcement officer where it is not readily apparent (e.g.: at night; member is in plainclothes; member is in an unmarked vehicle.)

A member shall not use ***force*** upon another individual unless:

- De-escalation tactics have been attempted and failed or such tactics are not feasible based on the totality of the circumstances and such force is necessary and proportionate to:
    - Effect the lawful arrest or detention of an individual;
    - Prevent the escape from custody of an individual;
    - Prevent imminent harm and the amount of force used is proportionate to the threat of imminent harm, while protecting the safety of the member(s) or others; or

Policy, continued

- Defend against an individual who initiates force against a member.

If deployed, ECW cycles shall be limited to the minimum number of deployments necessary and should last no longer than necessary to bring an individual under control.

When it is objectively reasonable that a subject is under the control of law enforcement, the use of force shall terminate.

Members shall adhere to the Duty to Intervene and Report mandates of General Order UOF-01, Use of Force.

When safe, and tactically feasible, members shall always provide appropriate medical response and proper medical aid to individuals who are exhibiting signs of, or complaining of, injury or illness, including following a use of force, which includes the use of an ECW, or other law enforcement action.

Definitions

Actively Resistant Individual: An individual who uses physical strength and/or body movement to resist a Department member. Examples of active resistance include pulling, turning, or walking away from an officer.

Aggravated Assaultive Individual (Serious Bodily Harm/Death): An individual who engages in conduct that is likely to produce death or serious bodily harm to a Department member or another person.

Assaultive Individual (Bodily Harm): An individual who attempts to injure a Department member or another person or engages in conduct that has the potential to injure a Department member or another person.

Compliant Individual: An individual who is fully cooperative with a Department member.

Deadly Force: Use of force intended to inflict, or reasonably be expected to cause, death or serious physical injury.

- Members may not use deadly force against an individual who poses only a danger to themselves.
- Deadly force shall not be used at any point in time when there is no longer an objectively reasonable belief than an individual currently and actively poses an immediate threat of serious bodily harm or death, even if deadly force would have been justified at an earlier point in time.

De-escalation Tactics: Proactive approaches to stabilize a law enforcement situation so that more time, options, and resources are available to gain voluntary compliance and/or reduce or eliminate the need for force. These approaches may include, but not be limited to:

- Verbal persuasion;
- Warnings;

Definitions, continued

- Slowing down the pace of an incident;
- Waiting out an individual;
- Creating distance between the member and a threat;
- Requesting additional resources, including, but not limited to, licensed medical or mental health professionals, as defined in M.G.L. c. 111 § 51 ½ (a), when appropriate, to address a potential medical or mental health crisis; and
- Issuing a summons as an alternative to arrest where feasible.

Drive Stun Deployment: In Drive Stun mode, the ECW is a pain-compliance facilitator rather than an electro-muscular disruptor. Drive stun occurs when the ECW is held against the subject, whether or not probes are deployed. Drive stun may be utilized in response to active resistance or assaultive behavior.

Electronic Control Weapon (ECW): A weapon that uses electricity to override voluntary motor responses or applies pain in order to gain compliance or overcome resistance. ECWs are designed to incapacitate without causing serious physical injury or death.

ECW Activation: Any time an ECW is turned on, exclusive of training and routine maintenance/readiness checks.

ECW Cycle: Occurs when probe deployment delivers energy to an individual.

Force: The amount of physical effort, however slight, required by police to compel compliance by an unwilling individual.

- Physically escorting or handcuffing an individual with minimal or no resistance does not constitute a use of force for the purposes of 550 CMR 6.03.
- Use of force ***does include*** the intentional pointing of a firearm or Electronic Control Weapon at an individual as an attempt to control that individual's movements, and the use of OC spray on an individual or directed towards an individual.

Laser Activation: The ECW is turned on, activating the light and/or laser beam. Laser activation may be utilized as a warning technique if drive stun deployment and/or probe deployment is objectively reasonable.

Definitions, continued

Less-Lethal Force: Any physical use of force, other than deadly force, to control, restrain, or overcome the resistance of another.

- Members are authorized to use less-lethal force in accordance with all applicable federal and state laws and regulations, the contents of General Order UOF-01 and the contents of this policy.

Objectively Reasonable: This term means that, in determining the necessity for and appropriate level of force, officers shall evaluate each situation in light of the known circumstances at the time, including, but not limited to, the seriousness of the crime, the level of threat or resistance presented by the subject, and the danger to the officer, subject, or community. The reasonableness of a particular use of force must be judged from the perspective of a reasonable officer on scene, rather than with the 20/20 vision of hindsight. Determining reasonableness of force must allow for the fact that police officers are often required to make instantaneous judgments in circumstances that are tense, uncertain and rapidly evolving. The force used must be reasonable under the circumstances known to the officer at the time force is used. *Graham v. Connor* 490 U.S. 386 (1989)

Passively Resistant Individual: An individual who is non-violent and uncooperative but does not use physical strength or body movement to resist a Department member and does not pose an immediate threat to the member or the public.

- A Member shall only use the amount of force necessary against an individual who is engaged in passive resistance to effect the lawful arrest or detention of said individual and shall use de-escalation tactics where feasible, including issuing a summons instead of executing an arrest where feasible.

Probe Deployment: In probe deployment mode, the ECW uses electricity to override voluntary motor responses. Probe deployment occurs when probes deploy from an ECW, whether or not the probes strike their intended target. This includes follow-up drive stuns when a single probe is attached to an individual. Probe deployment may be utilized in response to assaultive behavior.

Proper Medical Aid: Immediate first aid treatment, including CPR, administered on the scene of an incident/injury within the scope of the member's training. Additionally, medical aid includes the summoning of emergency medical services to assist in any condition or treatment that may escalate outside of the scope of the capabilities of the member(s) providing immediate first aid or requiring transportation to a medical facility based on the condition of the person receiving aid.

Reportable Incident: Shall include:

- The intentional pointing of a firearm or ECW at an individual;
- Application of force through the use of deadly or less-lethal weapons;
- On-duty discharge of any weapon outside of a training range specifically designed for that purpose;

Definitions, continued

- Off-duty discharge of a Department weapon outside of a training range specifically designed for that purpose;
- Department issued ECW activation, drive stun and/or probe, on or off duty, as defined in UOF-06 Electronic Control Weapons;
- Compliance or striking techniques are used;
- Use of OC spray on an individual or directed toward an individual; or
- Use of force which actually, or proximately, caused or is reported to have caused injury or death to another.

Sensitive Population Groups: Sensitive population groups include those who reasonably appear to be, or are known to be, children, elderly, medically infirm, intellectually disabled, pregnant, or users of a cardiac pacemaker.

Serious Bodily Injury: Injury that results in or involves a substantial risk of death, permanent or protracted disfigurement, or extended loss or impairment of the function of a body part or organ.

Warning Arc: The ECW is activated and the arc switch is depressed, activating the electrical arc. A warning arc may be utilized as a de-escalation or warning technique if drive stun deployment and/or probe deployment is objectively reasonable.

ECW Readiness

Department members issued and authorized to use a ECW shall:

- Ensure the ECW is carried in an approved holster on the side of the body opposite the service handgun;
  NOTE: members not assigned to uniformed duty may use other Department-approved holsters and carry the weapon consistent with Department training.
- Ensure the ECW is fully armed with the safety on in preparation for immediate use;
- Ensure the ECW cartridges are loaded in a manner consistent with training;
- Ensure cartridges are replaced following the manufacturer's expiration requirements;
- Ensure only manufacturer-approved battery power sources are used for the ECW;
- Prior to each regular tour of duty shift, confirm that the ECW is functioning properly by performing all tests as defined in training;
- Not make any modifications or repairs on the ECW unless authorized in writing by the Armorer; and
- TASER 7: Ensure battery packs are docked:
  - At least once every 30 days;
  - When the battery reaches 20% capacity or lower; or
  - Within 24 hours of an activation, as defined in General Order UOF-03, Use of Force Reporting.

Subject	Number
Electronic Control Weapons	**UOF-06**

Activation

In accordance with applicable federal and state laws and regulations, the contents of General Order UOF-01 Use of Force, and this policy, and when it is objectively reasonable to do so, Department members are authorized to utilize an ECW to arrest and/or detain an individual that has and/or continues to exhibit behavior that leads the member to believe the individual is actively resisting or assaultive and will resist being arrested or detained.

ECW Use of Force Response Table

If the subject is:	Then the response may include:
Actively Resistant	Laser Activation Warning Arc Drive Stun
Assaultive – Bodily Harm	Laser Activation Warning Arc Drive Stun Probe Deployment
Aggravated Assaultive – Serious Bodily Harm/Death	Laser Activation Warning Arc Drive Stun Probe Deployment NOTE: Department members are not required to use a weapon of less-lethal force if use of deadly force is objectively reasonable.

Situations in which the ECW may be activated in accordance with the above table include but are not limited to:

- When an individual uses force or violence against the member or another person(s);
- When an individual exhibits violent, threatening, or potentially violent behavior;
- When an individual actively resists an arrest or detention;
- When an individual flees in order to avoid arrest or detention in circumstances where the member would pursue on foot and physically effect the arrest or detention;
- When an individual expresses intent and has the means to commit suicide or inflict serious bodily harm to themselves or others and ECW activation does not create additional risk;
- To protect Department members or others against an aggressive animal; and
- In the course of Department-authorized training exercises or demonstrations.

Department members shall:

- Give the individual a warning prior to activating the ECW, unless doing so would place any member or person(s) at risk;

Activation, continued

- Adhere to the Department's training regarding warnings, which may include clear verbal warnings, display of the ECW, laser painting, display of a warning arc, or a combination thereof;
- When feasible, an announcement should be made to other members or personnel on the scene that an ECW is going to be activated;
- Not intentionally activate more than one ECW at a time against an individual;
- Be aware that an individual subjected to an ECW Cycle may not be able to respond to commands during or immediately following an ECW Cycle exposure;
- ECW cycles should be limited to the least number of exposures and should last no longer than necessary to bring an individual under control; Each 5-second cycle is considered an independent use of force and must be objectively reasonable and be documented in writing;
- Avoid continued ECW use as an attempt to facilitate compliance if circumstances indicate that drive stun deployment is ineffective as a pain-compliance technique;
- Be aware that pain compliance may not be effective against an individual in a mental health crisis state, under the influence of a mind-altering substance, or when extremely focused;
- Consider potential risk(s) to third-parties or bystanders when activating ECWs;
- Be aware that a subject's heavy clothing may impede the effectiveness of ECWs;
- Aim, to the degree possible, for the following target areas:
  - Lower center mass below the chest
  - Back
  - Legs

  Note: Consistent with training and to the extent possible, Department members should avoid sensitive areas such as the eyes, face, head, throat, neck, breasts, groin and genitals.

Department members shall *not* use the ECW:

- On individuals who passively resist as defined within this policy;
- On a handcuffed or secured detainee;
  EXCEPTION: ECW, in limited situations, may be used on a handcuffed or secured detainee if an individual exhibits overtly assaultive, self-destructive, or violently resistive behavior that cannot reasonably be controlled by other readily available means.
- In any environment where the member reasonably believes that a flammable, volatile, or explosive material is present, including but not limited to OC spray with volatile propellant, gasoline, natural gas, propane;
- When the individual is immersed or partially immersed in a body of water;
- In any situation where the member has a reasonable belief that the individual might fall resulting in death or serious physical injury, and the circumstances presented do not justify that risk; or

Activation, continued

- On individuals in physical control of a vehicle in motion (e.g., motor vehicles, trucks, motorcycles, ATVs, bicycles, scooters) unless exigent circumstances exist.

Sensitive Population Group

Department members shall be aware of general concerns when an ECW is used on a sensitive population group individual. Department members are not prohibited from using an ECW on sensitive population group individuals, but use is limited to those exceptional circumstances where the potential benefit of using the ECW (i.e., injury reduction) reasonably outweighs the risks and concerns.

ECW Post-Activation

After a probe deployment in which the probe(s) became embedded in the subject's body, Department Members shall seek medical attention for the individual and ensure that the embedded ECW probe(s) are removed by qualified medical personnel.

In any case of Drive Stun deployment or Probe deployment from an ECW on an individual, members shall:

- Transport the individual to an emergency care facility for evaluation and/or treatment if any of the following apply:
    - The individual requests medical attention or there is an obvious need for medical attention;
    - The ECW was deployed in a sensitive area (e.g., eye, face, head, throat, neck, breasts, groin, genitals);
    - The individual is part of a sensitive population group;
    - More than three ECW cycles were deployed on the individual or the ECW was deployed for continuous cycles amounting to 15 seconds or more; or
    - More than one ECW device has been deployed on an individual.
- Use restraint techniques that minimize risk of impairing a subject's respiration.
- Make reasonable efforts to protect the subject's privacy.

Internal Reporting

Department members who intentionally point an ECW at an individual or activate an ECW (drive-stun or probe deployment) shall:

- Adhere to General Order UOF-03, Use of Force Reporting;
- Report ECW activations to the Station Desk Officer of jurisdiction;
- Ensure ECW activations are documented within the Daily Administrative Journal/Department Records Management System; and
- TASER X2: Ensure that Station/Unit Commander is provided access to ECW for downloading purposes.
- TASER 7: Place the battery in a dock within 24 hours of a reportable incident and ensure data upload is completed.

<u>The involved member(s) shall:</u>

- Submit a SP-376 Use of Force Report within 24 hours of a reportable incident as defined in UOF-03; and

- TASER 7: Place the battery in a dock within 24 hours of a reportable incident and ensure the data upload is completed.

Internal Reporting, continued

Supervisors shall:

- Ensure involved member(s) submit a SP 376;
- Review every SP 376; and
- Forward reports to the Division Commander, through channels with findings and recommendations as to the necessity of further investigation of the incident.

Station/Unit Commander or Designee shall:

- Ensure that ECW data is downloaded per manufacturer instructions; and
- Ensure that data from ECW download is consistent with reports submitted by involved member(s).

External Reporting

The Use of Force Review Committee shall:

- Collect Department information regarding the use of ECW;
- Ensure the Executive Office of Public Safety and Security (EOPSS) *ECW Use Reporting Form* is completed and submitted as required by EOPSS in accordance with M.G.L. c. 140, § 131J and St. 2004, c. 170, §2;
- Forward a copy of the EOPSS *ECW Use Reporting Form* to the Deputy Superintendent.

Off-Duty Considerations

Members are ***not authorized*** to carry their Department issued ECW while off duty. When off-duty, members shall secure Department issued ECWs in a manner consistent with the securing of a firearm and in accordance with all applicable Massachusetts Laws. Members must ensure that Department issued ECWs are inaccessible to children and others.

Training

At least annually, all Department members authorized to carry weapons shall receive in-service training on the Department's UOF policies and demonstrate proficiency with all approved deadly weapons and ECW's issued to the member. The administration of the training shall be documented and records maintained by the State Police Academy (SPA). Training and proficiency testing shall be conducted by certified instructors.

Department members shall be trained in accordance with the lesson plan provided by the manufacturer approved by EOPSS in accordance with M.G.L. c. 140, § 131J.

Department members shall be trained in accordance with all applicable federal and state laws and regulations, the contents of General Order UOF-01, and the contents of this policy.

Subject	Number
Electronic Control Weapons	**UOF-06**

References

UOF-01 Use of Force;
UOF-03 Use of Force Reporting;
UOF-04 Use of Force Equipment;
SP 376 Use of Force Report;
501 CMR 8.00 *et seq.;*
550 CMR 6.00 *et seq*.;
M.G.L. c. 6E, § 14;
M.G.L. c. 140, § 131J and St. 2004, § 2;
MPAC: 1.1.4, 1.1.5, 1.1.6, 1.1.7, 1.1.9, 1.1.10, 1.1.11, 1.1.12;
Electronic Control Weapons in Massachusetts 2014, Executive Office of Public Safety and Security;
Executive Office of Public Safety and Security ECW Use Report;
International Association of Chiefs of Police (IACP) Electronic Controlled Weapon Model Policy, April 2010;
Police Executive Research Forum Electronic Control Weapon Guidelines, 2011;
Taser® Lesson Plan ;
TASER 7 CEW User Course (Version 22);
TASER Energy Weapon Master Instructor One Day Instructor Course Drill Booklet.

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
Rules & Regulations

Effective Date:	Number:
November 10, 2021	**Appendix "A"**
Subject: **DISCIPLINE GUIDELINES**	

Class

A	1. 2. 3.	***FIRST OFFENSE***: Suspension of not less than thirty (30) days up to and including termination. ***SECOND OFFENSE:*** Suspension of not less than ninety (90) days up to and including termination. ***THIRD OFFENSE:*** Termination.
B	1. 2. 3.	***FIRST OFFENSE***: Suspension of not less than five (5) days nor more than thirty (30) days. ***SECOND OFFENSE:*** Suspension of not less than ten (10) days nor more than sixty (60) days. ***THIRD AND SUBSEQUENT OFFENSE(S):*** Suspension of not less than thirty (30) days up to and including termination.
C	1. 2. 3.	***FIRST OFFENSE:*** Written reprimand up to and including suspension of not more than five (5) days. ***SECOND OFFENSE:*** Suspension of not less than one (1) day nor more than fifteen (15) days. ***THIRD AND SUBSEQUENT OFFENSE(S):*** Suspension of not less than fifteen (15) days up to and including termination.
D	1. 2. 3.	***FIRST OFFENSE:*** Written reprimand up to and including suspension of not more than two (2) days. ***SECOND OFFENSE:*** Written reprimand up to and including a suspension of not more than five (5) days. ***THIRD AND SUBSEQUENT OFFENSE(S):*** Suspension of not less than ten (10) days up to and including termination.

INTERPRETATIVE NOTES FOR APPENDIX "A"

1. When determining the number of prior offenses under the Guideline, the Trial Board shall consider only those offenses, which occurred on or after March 19, 1997, for which the member was found guilty and which were scheduled in a Class equivalent to or, superior to, the Class of the subject offense; provided however, a member's complete and entire disciplinary history including all offenses, if any, committed before March 19, 1997, shall be considered as aggravating or mitigating factors, as the case may be, when recommending discipline.

2. The Trial Board may recommend loss of accrued vacation/personal/holiday time as an alternative to suspension. Such recommendation shall not be considered a departure from the Guideline provided the number of days so recommended is consistent with the Guideline.

3. Not-withstanding the Class Schedule, members may be charged and prosecuted for any action violating a Rule and/or Regulation.

4. Rules and Regulations which have been ranked within the Class Schedule (i.e., A-B-C-D) denote violations which, predicated on the circumstances, encompass a broad scope of behavior ranging from the most egregious to the most negligible. Ranked Articles shall be scheduled in accordance with Rule 6.4.1 except as otherwise authorized by Rule 6.9.

APPENDIX "A" DISCIPLINE GUIDELINES

CLASS SCHEDULE

SECTION #	*SECTION TITLE*	*CLASS*
1.0	REGULATIONS FOR THE GOVERNANCE OF THE MASSACHUSETTS STATE POLICE……	N/A
1.1	AUTHORIZATION AND SEVERABILIY……..	N/A
1.2	INTRODUCTION……..	N/A
1.2.1	……	N/A
1.2.2	……	N/A
1.2.3	……	N/A
1.2.4	……	D
1.2.5	……	D
1.2.6	……	D
1.3	**CODE OF ETHICS**……..	N/A
1.3.1	……	D
1.3.2	……	D
1.3.3	……	D
1.3.4	……	B
1.3.5	……	C
1.3.6	……	D
1.3.7	……	D
1.3.8	……	D
1.3.9	……	N/A
1.3.10	……...	B
2.0	**ORGANIZATIONAL VALUES**……	N/A
3.0	**REGULATIONS ESTABLISHING THE DUTIES OF MEMBERS**…….	N/A
3.1	SUPERINTENDENT…….	N/A
3.2	DEPUTY SUPERINTENDENT……	N/A
3.3	STAFF OFFICERS……	N/A
3.4	COMMISSIONED OFFICERS…….	N/A
3.5	NONCOMMISSIONED OFFICERS……	N/A
3.6	COMMAND RESPONSIBILITY…….	N/A
3.7	SUPERVISORY MEMBERS……	N/A
3.7.1	……	C
3.7.2	……	C
3.7.3	……	C
3.7.4	……	C
3.7.5	……	C
3.7.6	……	C
3.7.7	……	C
3.7.8	……	D
3.7.9	……	C
3.7.10	……	N/A
3.7.11	……	C
3.8	**MEMBERS APPOINTED UNDER M.G.L. c.22C**……...	N/A
3.8.1	……	C
3.8.2	……	B-C
3.8.3	……	A-B-C-D
3.8.4	……	A-B-C-D
3.8.5	……	A-B-C-D
3.8.6	……	D
3.8.7	……	N/A
3.8.8	……	C
3.8.9	……	N/A
3.8.10	……	C

3.9	**CIVILIAN EMPLOYEES**……..	N/A
4.0	**TITLE AND RANK, PAYROLL, PROMOTIONS**…….	N/A
5.0	**RULES OF CONDUCT**……..	N/A
5.1	VIOLATION OF RULES……..	A-B-C-D
5.1.1	……	D
5.2	UNBECOMING CONDUCT…….	B
5.2.1	……	B
5.2.2	……	A-B-C
5.3	GENERAL CONDUCT…….	B
5.4	CONFORMANCE TO LAWS……	N/A
5.4.1	……	A-B-C
5.4.2	……	N/A
5.4.3	……	C
5.4.4	……	C
5.4.5	……	C
5.5	REPORTING FOR DUTY…….	N/A
5.5.1	……	D
5.5.2	……	C
5.5.3	……	C
5.6	NEGLECT OF DUTY……	B-C
5.7	FICTITIOUS ILLNESS OR INJURY REPORT……..….	C
5.8	UNSATISFACTORY PERFORMANCE…….	N/A
5.8.1	……	C-D
5.8.2	……	A-B-C-D
5.8.3	……	B
5.9	EMPLOYMENT OUTSIDE OF THE DEPARTMENT……	N/A
5.9.1(1)	……	D
5.9.1(2)	……	B-C
5.9.2	……	B
5.9.3	……	N/A
5.9.4	……	C
5.10	ALCOHOLIC BEVERAGES AND DRUGS……	N/A
5.10.1	……	C
5.10.2	……	B
5.10.3	……	B
5.10.4	……	B
5.11	USE OF TOBACCO, GUM AND OTHER FOREIGN OBJECTS……..	N/A
5.11.1	……	A
5.11.2	……	C
5.11.3	……	C
5.12	INSUBORDINATION……...	N/A
5.12.1	……	B
5.12.2	……	A
5.12.3	……	B
5.13	CONFLICTING OR ILLEGAL ORDERS……	N/A
5.13.1	……	N/A
5.13.2	……	B
5.13.3	……	N/A
5.14	GIFTS, GRATUITIES, BRIBES OR REWARDS…….	A
5.14.1	……	A
5.15	ABUSE OF POSITION……..	N/A
5.15.1	……	A
5.15.2	……	B-C
5.15.3	……	B-C
5.15.4	……	A
5.15.5	……	A
5.15.6	……	A
5.16	ENDORSEMENTS AND REFERRALS……	B-C

5.17	IDENTIFICAITON……	N/A
5.17.1	……	D
5.17.2	……	N/A
5.17.3	……	D
5.17.4	……	D
5.18	PAYMENTS OF DEBTS……...	N/A
5.18.1	……	D
5.18.2	……	D
5.18.3	……	C
5.19	POLITICAL ACTIVITY……	N/A
5.19.1	……	B-C
5.19.2	……	B-C
5.19.3	……	B-C
5.19.4	……	B-C
5.19.5	……	B-C
5.19.6	……	B-C
5.19.7	……	B-C
5.20	CIVIL ACTIONS……...	B-C
5.21	RESIDENCE (1ST SENTENCE)……	B-C
5.21	RESIDENCE (2ND SENTENCE)……..	D
5.22	TELEPHONE…….	D
5.23	DISSEMINATION OF INFORMATION……..	N/A
5.23.1	……	N/A
5.23.2	……	C
5.23.3	……	B
5.23.4	……	A
5.23.5	……	A
5.23.6	……	C
5.23.7	……	C
5.23.8	……	D
5.23.9	……	C
5.23.10	……	C
5.24	INTERVENTION……..	N/A
5.24.1	……	A
5.24.2	……	C
5.25	ABUSE OF PROCESS……..	A
5.26	USE OF EQUIPMENT……..	N/A
5.26.1	……	B
5.26.2	……	A
5.26.3	……	D
5.26.4	……	D
5.26.5	……	C
5.26.6	……	D
5.26.7	……	D
5.26.8	……	B
5.26.9	……	C
5.27	TRUTHFULNESS…….	N/A
5.27.1	……	B
5.27.2	……	A
5.27.3	……	A
5.28	OFFICIAL CORRESPONDENCE AND OFFICIAL BUSINESS……	N/A
5.28.1	……	D
5.28.2	……	C
5.29	INTERCESSION FOR MEMBERS…….	N/A
5.29.1	……	C
5.29.2	……	B
5.29.3	……	A

6.0	**REGULATIONS ESTABLISHING DISCIPLINARY PROCEDURES AND TEMPORARY RELIEF FROM DUTY**…….……	N/A
6.1	TEMPORARY RELIEF FROM DUTY…….	N/A
6.2	DUTY STATUS HEARING……..	N/A
6.3	LETTER OF COUNSELING…….	N/A
6.4	CHARGES AND DISPOSITION WITHOUT HEARING……	N/A
6.5	HEARING ON CHARGES……	N/A
6.6	DEPARTMENTAL PROSECUTOR…….	N/A
6.7	TRIAL BOARD…….	N/A
6.8	DEPUTY SUPERINTENDENT'S ACTION……	N/A
6.9	JUDGEMENTS AND DISCIPLINE…….	N/A
7.0	**REGULATIONS ESTABLISHING ENLISTMENT AND DISCHARGE….**	N/A
7.1	ENLISTMENT……..	N/A
7.2	DISCHARGE AND RESIGNATION…….....	N/A
8.0	**REGULATIONS ESTABLISHING THE BOARD ON CLAIMS……..**	N/A
8.1	BOARD ON CLAIMS……..	N/A
9.0	**REGULATIONS ESTABLISHING EXAMINATION APPEAL……**	N/A

Promulgated by: Christopher S. Mason, Colonel/Superintendent

Department of State Police
Rules & Regulations

Effective Date:	Number:
November 10, 2021	**Article 1**

Subject:
REGULATIONS FOR THE GOVERNANCE OF THE STATE POLICE

1.0 REGULATIONS FOR THE GOVERNANCE OF THE STATE POLICE

1.1 AUTHORIZATION AND SEVERABILITY

For the purpose of these Rules and Regulations the Massachusetts Department of State Police shall hereinafter be referred to as the "Massachusetts State Police". Uniformed members shall hereinafter be referred to as "members" or “sworn members.”

The Massachusetts State Police's Rules and Regulations are issued pursuant to Massachusetts General Law Chapter 22C. These Rules and Regulations cancel and supersede all previous Massachusetts State Police Rules and Regulations. Causes of actions arising from events transpiring prior to March 19, 1997, shall be governed by Rules and Regulations then in effect.

If any article, section, sub-section, sentence, clause, or phrase of the Rules and Regulations is for any reason held to be unconstitutional, contrary to law, or otherwise inoperative, such decision shall not affect the validity of any other part of these Rules and Regulations.

1.2 INTRODUCTION

In the United States it is essential that the Criminal Justice System upon which public safety depends be administered in a manner which promotes public respect, confidence and acceptance.

The problems associated with the delivery of police services are many, as they reflect the complex interactions and changes of modern society. Accordingly, rules cannot be drafted that shall prescribe, in specific detail, the manner in which all duties of Massachusetts State Police members are to be performed. Consequently, all members should be guided in their decision-making processes by subscribing to certain fundamental principles.

1.2, continued These principles are as follows:

1.2.1 Members shall endeavor to elevate the standing of the Law Enforcement profession in the public mind and to strengthen public confidence in the Massachusetts State Police.

1.2.2 Members shall encourage all other members of the Massachusetts State Police to fully appreciate the responsibilities of their office.

1.2.3 Members shall endeavor to develop and maintain the public's support and cooperation.

1.2.4 Members shall promote the concept of teamwork for the benefit of all.

1.2.5 Members shall strive for full coordination of effort in all official relationships.

1.2.6 Members shall provide high quality problem solving and community-oriented police services.

1.3 CODE OF ETHICS

All members and civilian employees shall abide by this code of ethics which is a reflection of the organizational values of the Massachusetts State Police and is adopted as a general performance standard for all members and civilian employees.

1.3.1 We shall respect the diversity of, and be sensitive to, all people.

1.3.2 We shall accept our responsibility to the public by being punctual in our engagements and expeditious in the performance of duty.

1.3.3 We shall regard our office as a public trust and, in the discharge of our duties, be mindful of our primary obligations to serve the public efficiently and effectively.

1.3.4 We shall administer the law in a just, impartial, and reasonable manner, affording the same reasonable treatment to all cases.

1.3.5 We shall recognize the limitations of our authority and at no time use the power of our office for our personal advantage.

1.3.6 We shall be true to our obligations as custodians of public property.

1.3.7 We shall not diminish our integrity or limit our effectiveness by accepting gratuities or favors from persons, businesses, corporations, or other entities.

1.3, continued

1.3.8 We shall cooperate fully with other public officials to assure the safety and general welfare of the public. We shall not permit jealousies or personal differences to influence our ability to cooperate with others in our official business.

1.3.9 We shall add to our effectiveness by enhanced training, diligent study, and sincere attention to self-improvement, including physical readiness. We shall welcome the opportunity to disseminate practical and useful information relating to matters of the public's safety and welfare.

1.3.10 We shall bear faithful allegiance to our government and be loyal to our profession. We shall accept as an obligation our responsibility to support the Constitutions of the United States and the Commonwealth of Massachusetts.

1.3.11 We shall fervently seek out and report the truth.

Promulgated by: Christopher S. Mason, Colonel/Superintendent

Department of State Police
Rules & Regulations

Effective Date:	Number:
November 10, 2021	**Article 2**
Subject:	
ORGANIZATIONAL VALUES	

2.0 ORGANIZATION VALUES

The value statements of the Massachusetts State Police are:

2.1 Maintenance of the highest standards of integrity and ethics.

2.2 Excellence and teamwork in the performance of duty.

2.3 Protection of Constitutional Rights.

2.4 Problem solving for continuous improvement.

2.5 Continuous planning for the future.

2.6 Performing public service and law enforcement tasks so as to provide leadership to the police profession.

Promulgated by: Christopher S. Mason, Colonel/Superintendent

Department of State Police
Rules & Regulations

Effective Date:	Number:
November 10, 2021	**Article 3**

Subject:

REGULATIONS ESTABLISHING THE DUTIES OF SWORN MEMBERS AND CIVILIAN EMPLOYEES

3.0 REGULATIONS ESTABLISHING THE DUTIES OF MEMBERS

To attain the Massachusetts State Police organizational goals and to implement the regulations of the Massachusetts State Police, the following duties are established for the Superintendent, Deputy Superintendent, Supervisory members, other uniformed members appointed under M.G.L. c. 22C, and civilian employees of the Massachusetts State Police.

For the purpose of this Article, the term "member" shall refer only to sworn members. The term "employee" shall refer to both sworn members and civilian employee(s).

3.1 SUPERINTENDENT

The Superintendent of the Massachusetts State Police shall hold the rank of Colonel and shall be the executive and administrative officer of the Massachusetts State Police. They shall promulgate all Rules, Regulations, Policies, Procedures, Orders, and Directives governing the Massachusetts State Police including, but not limited to, discipline, organization, government, administration, training, and compensation.

3.2 DEPUTY SUPERINTENDENT

A Lieutenant Colonel shall be designated by the Colonel/Superintendent as the Deputy Superintendent and shall be the second-in-command of the Massachusetts State Police. They shall exercise such authority and supervision over functions of the Massachusetts State Police as the Colonel may assign and during the absence of or when so designated by the Colonel/Superintendent shall perform the official duties of the Colonel/Superintendent.

3.3 STAFF OFFICERS

Staff Officers, with the exception of the Colonel/Superintendent, shall be appointed by the Colonel/Superintendent and shall exercise such authority and supervision over the functions of the Massachusetts State Police as maybe assigned.

3.3.1 The term Staff Officer shall include the following ranks:

- Colonel/Superintendent
- Lieutenant Colonel/Deputy Superintendent
- Lieutenant Colonel
- Major

3.3.2 The Colonel/Superintendent shall fill vacancies in the ranks of Lieutenant Colonel/Deputy Superintendent, Lieutenant Colonel and Major with those officers who are eligible for such promotions. Officers so appointed may be returned to their previous rank, or to the rank of Captain, at the discretion of the Colonel/Superintendent.

3.4 COMMISIONED OFFICERS

A Commissioned Officer shall exercise such authority and supervision over the functions of the Massachusetts State Police as may be assigned by senior supervisory members or proper authority.

3.4.1 The term Commissioned Officer shall include the following ranks:

- Detective Captain
- Captain
- Detective Lieutenant
- Lieutenant

3.4.2 The Colonel/Superintendent shall fill vacancies in the ranks of Detective Captain from officers holding the rank of Captain and shall fill vacancies in the rank of Detective Lieutenant from officers holding the rank of Lieutenant. Any officer so appointed to the rank of Detective Captain or Detective Lieutenant on or after July 1, 1994, may be returned to their previous rank at the discretion of the Colonel/Superintendent.

3.5 NON-COMMISIONED OFFICERS

A Non-commissioned Officer shall exercise such authority and supervision over the functions of the Massachusetts State Police as may be assigned by senior supervisory members or proper authority.

3.5.1 The term Non-commissioned Officer shall include the following rank:

- Sergeant

3.6 COMMAND RESPONSIBILITY

Unless otherwise ordered by the Colonel/Superintendent or Lieutenant Colonel/Deputy Superintendent, the senior Staff Officer, Commissioned Officer, Non-commissioned Officer or other senior member present shall be in command.

3.6.1 Senior member status shall be determined by:

- Rank
- Length of service in rank
- As names in order of appointment or promotion

3.6.2 At the scene of a homicide, suspicious death, suicide, or unattended death, the member designated by the Division of Investigative Services Commander of jurisdiction shall assume immediate command. Orders concerning the investigation shall be given by no member of the Massachusetts State Police except the Colonel/Superintendent or a senior supervisory member within the Division of Investigative Services.

3.7 SUPERVISORY MEMBERS

Supervisory members shall include Staff Officers, Commissioned Officers, and Non-Commissioned Officers, and shall be responsible for adherence to all State Police Rules, Regulations, Policies, Procedures, Orders, and Directives. They are responsible and accountable for the maintenance of discipline and shall provide leadership, supervision, and continuous training and serve as an example to ensure the efficiency of all operational areas. They have the responsibility to positively influence other members and to motivate them to perform at a high level of efficiency. They have the responsibility for the performance of all members placed under them and, while they can delegate authority and functions, they cannot delegate responsibility. Supervisory members shall:

3.7, continued

3.7.1 Lead, direct, train, supervise, and evaluate employees in their assigned duties.

3.7.2. Provide leadership and guidance in developing loyalty to the Massachusetts State Police and dedication to the police profession.

3.7.3 Perform specific duties and functions as assigned by senior supervisory employees or proper authority.

3.7.4 Support employees who are properly performing their duty, deal fairly and equitably with all employees and, when necessary, correct them in a dignified manner.

3.7.5 Cooperate with all Massachusetts State Police employees and other governmental agencies.

3.7.6 Recommend remedial or disciplinary action for inefficient, incompetent, or unsuitable employees.

3.7.7. Ensure that Rules, Regulations, Policies, Procedures, Orders, and Directives of the Massachusetts State Police are enforced and adhered to by employees under their charge.

3.7.8 Remain accountable for any failure, misconduct, or omission by employees under their charge.

3.7.9 Report violations of law committed by employees, through channels, to the Colonel/Superintendent. Report violations of Massachusetts State Police Rules, Regulations, Policies, Procedures, Orders, and Directives committed by employees, through channels, to the Division Commander and as appropriate to the Colonel/Superintendent.

3.7.10 During any temporary absence or disability of a member of the Massachusetts State Police, which prevents the performance of their duties, the command shall devolve to the next higher rank, unless otherwise ordered by a senior supervisory member or proper authority from within the same Division or Troop/Section/Unit.

3.7.11 Any unusual occurrence that may have an adverse impact upon the Massachusetts State Police shall be reported, through channels, to the Division Commander and, as appropriate, to the Colonel/Superintendent.

3.7, continued

3.7.12 Any unusual occurrence that may result in a question of the Department's liability and/or result in heightened community or media interest shall be reported, through channels, to the Division Commander and, as appropriate, to the Colonel/Superintendent.

3.8 **UNIFORMED MEMBERS APPOINTED UNDER M.G.L. c. 22C**

All uniformed members appointed under M.G.L. c. 22C shall conduct themselves, at all times, in a fashion consistent with all Rules, Regulations, Policies, Procedures, Orders, and Directives. Members shall:

3.8.1 Render the highest order of police service to the citizens.

3.8.2 Obey all laws and promptly execute all lawful orders, including orders from a Supervisory member relayed through a member/employee of equal/lesser position.

3.8.3 Know and conform to all applicable law, State Police Rules, Regulations, Policies, Procedures, Orders, and Directives.

3.8.4 Receive, record, and respond to all complaints and requests for service.

3.8.5 Provide security and care for all persons and property coming into their custody.

3.8.6 Maintain a military-like bearing and courtesy at all times.

3.8.7 Notify the appropriate Division Commander, in writing through channels, when aggrieved by treatment or actions of a senior employee not amounting to a specific violation of any Rule, Regulation, Policy, Procedure, Order, or Directive. Such complaint shall then be forwarded promptly, through channels, to the Office of the Colonel/Superintendent with recommendations.

3.8.8 Be on-duty or subject to recall twenty-four hours a day. A member may be recalled from leave or vacation when necessity demands. On hearing of a state of emergency, as declared by the Governor, all members (excluding personnel on suspension, injury, or other approved leaves) shall immediately contact their duty assignment supervisor, or other supervising officer within the chain-of-command, for specific instructions.

3.8.9 All members, without exception and regardless of rank, assignment, or duties regularly performed, shall be subject to all duties of the Department, including, but not limited to, emergency duties.

3.8, continued

3.8.10 During the period immediately following a member's date of initial enlistment, when the probationary member is being trained by a senior member ("break in"), no such probationary member shall wear a State Police uniform or part(s) thereof while commuting to and from their duty assignment in a private vehicle unless authorized by the Troop Commander.

3.9 **CIVILIAN EMPLOYEES**

Civilian employees shall perform their assigned duties promptly and efficiently and shall:

3.9.1 Obey all laws and execute all lawful orders/directives. Clarification of conflicting/illegal-orders/directives received by a civilian employee shall be addressed through their immediate supervisor. If the conflicting/illegal-order/directive is received from their immediate supervisor then clarification shall be sought through a higher level supervisor within their chain of command.

3.9.2 Be bound by those Rules, Regulations, Policies, Procedures, Orders, and Directives of the State Police as determined by the Colonel/Superintendent.

3.9.3 Follow orders/directives from a supervisory member, supervisor or manager relayed through a member/employee of equal/lesser position.

3.9.4 Be known as Trainees upon beginning recruit training at the Massachusetts State Police Academy.

3.9.5 Upon hearing of a state of emergency, as declared by the Governor, immediately contact their duty assignment supervisor, or other supervising officer within the chain-of-command, for specific instructions, if said employee is designated as Emergency or Rotating Emergency Personnel (excluding personnel on suspension, injury, or other approved leaves).

3.9.6 Abide by the applicable Code of Conduct or Commonwealth Employment Standards established by the Commonwealth of Massachusetts Human Resources Division and the employees Collective Bargaining Agreement.

3.9.7 Be attired in a manner appropriate to the employee's job responsibilities and work unit of the employee.

References: MPAC: 11.4.5, 12.1.3, 26.1.1

Promulgated by: Christopher S. Mason, Colonel/Superintendent

Department of State Police
Rules & Regulations

Effective Date:	Number:
November 10, 2021	**Article 4**
Subject:	
TITLE AND RANK, PAYROLL, PROMOTIONS	

4.0 TITLE AND RANK, PAYROLL, PROMOTIONS

4.1 The order of titles and ranks in the Massachusetts State Police shall be as follows:

- Colonel/Superintendent
- Lieutenant Colonel/Deputy Superintendent
- Lieutenant Colonel
- Major
- Detective Captain
- Captain
- Detective Lieutenant
- Lieutenant
- Sergeant
- Trooper

4.2 The pay scale for the members and trainees of the Department of State Police appointed under the provisions of M.G.L. c. 22C is fixed and established in accordance with the following titles and ranks:

- Colonel/Superintendent
- Lieutenant Colonel/Deputy Superintendent
- Lieutenant Colonel
- Major
- Detective Captain
- Captain
- Detective Lieutenant
- Lieutenant
- Sergeant
- Trooper First Class
- Trooper
- Trainee

4.3 In the event the Colonel/Superintendent elects to fill a vacancy or vacancies s/he shall issue a Personnel Order pronouncing his/her intention to do so, and shall thereafter fill such vacancy or vacancies within sixty days after such Order is issued.

4.4 The Colonel shall promote individuals to promotional vacancies within sixty days, unless the Colonel, as executive and administrative head of the Massachusetts State Police in charge of the administration and organization thereof, issues a written order to the Division of Administrative Services within sixty days specifying that one or more of the following reasons exists which shall prevent the filling of such vacancies in the near future:

- The abolishment and/or consolidation of a division, bureau, section or unit of the Massachusetts State Police;
- Insufficient funding as appropriated by the General Court for the administration, organization, government, training, compensation,equipment, and maintenance of the Massachusetts State Police; or
- The assignment, reassignment or transfer of any uniformed member within or among a division or divisions of the Massachusetts State Police, and/or the staffing needs of any such division or divisions with consideration given to any completed or ongoing staffing study and/or any change in duties within a particular rank.

4.4.1 No orders issued by the Colonel pursuant to Rule 4.4 shall continue in effect for more than 180 days, unless the Colonel issues a new order to the Division of Administrative Services stating the specific reasons for extending such order.

Promulgated by: Christopher S. Mason, Colonel/Superintendent

Department of State Police
Rules & Regulations

Effective Date:	Number:
November 10, 2021	**Article 5**
Subject:	
RULES OF CONDUCT	

5.0 RULES OF CONDUCT

For the purpose of this Article, the term "member" shall refer only to sworn members. Civilian employee applicability shall be specifically stated.

5.1 VIOLATION OF RULES

Members shall not commit, nor cause to be committed, any act(s) or omit any act(s) which constitute(s) a violation of any Massachusetts State Police Rule, Regulation, Policy, Procedure, Order, or Directive.

5.1.1 All members and civilian employees of the State Police are required to familiarize themselves with the Rules, Regulations, Policies, Procedures, Orders, and Directives as may be issued or established by the Colonel/Superintendent. Members and civilian employees are also required to familiarize themselves with Orders and Directives as may be issued or established by senior supervisory members or proper authority.

5.2 UNBECOMING CONDUCT

Members shall conduct themselves at all times in such a manner as to reflect most favorably upon themselves and the Massachusetts State Police. Conduct unbecoming shall include that which brings the Massachusetts State Police into disrepute or reflects discredit upon the person as a member of the Massachusetts State Police, or that which impairs the operation, efficiency, or effectiveness of the Massachusetts State Police or the member.

5.2.1 Members shall not associate with individuals they know or should know are engaged in criminal activities unless in the performance of duty or upon official police business.

5.2.2 Members shall not frequent or remain at any place where they know or should know criminal activity is occurring unless in the performance of their duty or upon official police business.

5.3 GENERAL CONDUCT

Members shall maintain a level of conduct in their personal and business affairs which is in keeping with the highest standards of the law enforcement profession. Members shall not participate in any act which impairs their ability to perform as members of the State Police or causes the State Police to be brought into disrepute.

5.4 CONFORMANCE TO LAWS

5.4.1 Members shall obey all laws of the United States and of any country, state, or local jurisdiction in which the members are present.

5.4.2 A finding of responsible, continuance without a finding, or conviction due to alleged violation(s) of any law shall be prima facie evidence of a violation of this section.

5.4.3 Members who have been arrested or indicted, members against whom a criminal complaint, restraining order, or warrant for arrest has issued, and members who know or have reason to believe that they have been identified as a suspect in any criminal investigation shall notify their duty assignment supervisor forthwith of said incident or belief. Members are further required to provide a copy of any order modifying any previously issued permanent or temporary court order.

5.4.4 Members must possess a valid unrestricted Massachusetts driver’s license. Members who know or have reason to believe that their driver's license has expired, or has been suspended, revoked, or restricted shall notify their duty assignment supervisor forthwith. For the purposes of this Article, a corrective lens requirement shall not be considered a restriction.

5.4.5 Members must possess a valid unrestricted Massachusetts firearms license. Members who know or have reason to believe that their firearms license has expired, or has been suspended, revoked or restricted shall notify their duty assignment supervisor forthwith.

5.5 REPORTING FOR DUTY

5.5.1 Members shall report for duty at the time and place required by assignment or orders and shall be physically and mentally fit to perform their duties. They shall be properly equipped, attired, and cognizant of information required for the proper performance of duty so that they may immediately assume their duties as required by Massachusetts General Laws and Massachusetts State Police Rules, Regulations and Policies. A notice issued by any court shall constitute an order to report for duty under this section.

5.5, continued

5.5.2 Members shall perform any law enforcement duty that may be required of them by any senior member or proper authority. This shall be in addition to the specific duties and responsibilities previously assigned by the provisions of any State Police Rule, Regulation, Policy, Procedure, Order, or Directive.

5.5.3 A member assigned to a patrol or post shall not leave the patrol or post except for police necessity or personal necessity. If required to quit such patrol or post, members shall first receive permission to leave from their duty assignment supervisor or proper authority.

5.6 NEGLECT OF DUTY

Members shall not engage in any activities or conduct any personal business or affairs which would cause them to neglect or be inattentive to duty.

5.7 FICTITIOUS ILLNESS OR INJURY REPORT

Members shall not feign illness or injury, falsely report themselves ill or injured, or otherwise deceive or attempt to deceive any member of the State Police as to the condition of their health or their need for sick leave.

5.8 UNSATISFACTORY PERFORMANCE

5.8.1 Members shall maintain sufficient competency to properly perform their duties and assume the responsibilities of their positions. Members shall perform their duties in such a manner as will maintain the highest professionally accepted performance standards in carrying out the functions and objectives of the State Police.

5.8.2 Unsatisfactory performance may be demonstrated by a lack of knowledge of the application of laws required to be enforced; an unwillingness or inability to perform assigned tasks; the failure to conform to work standards established for the member's rank, title, or position; the failure to take appropriate action on the occasion of a crime, disorder, or other condition deserving State Police attention; or by an absent without leave.

5.8.3 In addition to other indicators of unsatisfactory performance, repeated infractions of State Police Rules, Regulations, Policies, Procedures, Orders, Directives or any combination of such infractions shall be considered prima facie evidence of unsatisfactory performance.

5.9 EMPLOYMENT OUTSIDE OF THE DEPARTMENT

5.9.1 Members may engage in off-duty employment subject to the following limitations:

- Such employment shall not interfere with the member's State Police employment; and
- Members shall refer to the Outside Employment Guide located in the State Police document management system and electronically submit a written request for off-duty employment through channels to the Colonel/Superintendent whose approval must be granted prior to engaging in any such off-duty employment.

5.9.2 Such employment shall not create any conflict of interest or violate M.G.L. c. 268A or any other law.

5.9.3 Approval may be denied at the discretion of the Colonel/Superintendent when it is determined that outside employment may present a conflict of interest, or it may:

- Render the member unavailable for an emergency;
- Physically or mentally exhaust the member to the point that their performance may be affected;
- Require special consideration be given to scheduling of the member's regular duty hours and/or court related appearances;
- Bring the member and/or the State Police into disrepute; or
- Impair the operation, efficiency, or effectiveness of the State Police.

5.9.4 Members who want to act as officials; judges or referees at public competitions or exhibitions shall refer to the Outside Employment Guide located in the State Police document management system and electronically submit a written request through channels to the Colonel/Superintendent for approval and must be granted such approval prior to engaging in any such activity.

5.10 ALCOHOLIC BEVERAGES

5.10.1 Members shall not, nor shall they permit, any person, including any member, to store or bring into any State Police facility or vehicle alcoholic beverages or controlled substances except that which is held as evidence or in the course of official duties, unless authorized by the Colonel/Superintendent.

5.10.2 Members shall not possess or use any controlled substance except when prescribed by a licensed medical practitioner for a legitimate medical purpose. When a controlled substance is prescribed that may impair the member's ability to perform their official duties, said member shall notify their duty assignment supervisor forthwith.

5.10.3 Members shall not consume alcoholic beverages while in uniform.

5.10, continued

5.10.4 Members shall not consume alcoholic beverages while on-duty except in the performance of duty and while acting under specific orders from a supervisory member or proper authority. Members shall not appear for duty, or be on-duty, while under the influence of alcoholic beverage(s) to any degree whatsoever, or with an odor of any alcoholic beverage(s) on their breath.

5.11 USE OF TOBACCO, GUM, AND OTHER FOREIGN OBJECTS

5.11.1 In accordance with M.G.L. c. 22C, no member or trainee appointed or hired after January 1, 1988 shall smoke any tobacco product. No member in violation of this Article shall continue in employment with the Massachusetts State Police.

5.11.2 No member or civilian employee shall smoke any tobacco product or possess any lit tobacco product in any Departmental building. No member or civilian employee shall smoke any tobacco product or possess any lit tobacco product in any Department vehicle, unless the vehicle is assigned to the member or employee and the member or employee is alone in said vehicle.

5.11.3 Members, when in uniform, shall not use tobacco, chew gum, or have any foreign object protruding from the mouth when they are:

- In view of the public; and/or
- In formation.

5.12 INSUBORDINATION

5.12.1 Members shall promptly obey any lawful order conveyed to them by any senior member or proper authority. For the purpose of this Article an order can be written or verbal.

5.12.2 Members shall not assault, strike, threaten, draw or lift up any weapon, or feign violence against any employee of the Massachusetts State Police.

5.12.3 Members shall not use threatening or insulting language or behave in any insubordinate or disrespectful manner toward any employee of the Massachusetts State Police.

5.13 CONFLICTING OR ILLEGAL ORDERS

5.13.1 Members who are given an order which may be in conflict with any Rule, Regulation, Policy, Procedure, Order, or Directive shall inform the issuing senior member or proper authority of the conflict. Unless the senior member or proper authority alters or retracts their order, said order shall stand. Under these circumstances, the responsibility for the conflict shall rest solely on the senior member or proper authority issuing said order.

5.13.2 Members shall not obey any order which they know or should know would require them to commit an act in violation of law. Any member who is given an order which they believe in good faith would result in a violation of law, shall inform the issuing senior member or proper authority of the possible violation, and if the order stands or, as revised, still calls for an act in violation of law, the member shall be allowed reasonable time to confer with a more senior supervisory member or proper authority within their Division. If after conferring with such senior supervisory member or proper authority, the order is not overturned, and the member refuses to obey such order, the member shall be accountable for any violations of these Articles.

5.13.3 Whenever there seems to be a conflict, or doubt as to the meaning, of written Massachusetts State Police Rules, Regulations, Policies, Procedures, Orders, or Directives, application shall be made in writing through channels to the Colonel/Superintendent for an explanation or possible correction.

5.14 GIFTS, GRATUITIES, BRIBES, OR REWARDS

In accordance with M.G.L. c. 22C, any member who directly or indirectly receives a reward, gift, or gratuity on account of his official services shall be subject to criminal sanctions and discharge from office. Awards of plaques, citations, or other articles of appreciation recognizing meritorious service or accomplishment that have no significant monetary value are not contemplated by this Rule.

5.14.1 Members shall not solicit or accept from any person, business, corporation or other entity or organization any gift (including but not limited to money, property whether tangible or intangible, food, beverage, loan, promise, service, entertainment, or any other thing or service of value) for the direct or indirect benefit of said member or the Massachusetts State Police if it may be reasonably inferred that the person, business, or organization:

- Seeks to influence action of an official nature or seeks to affect the performance or non-performance of an official duty; or
- Has an interest which may be substantially affected, directly or indirectly, by the performance or non-performance of an official duty.

5.15 ABUSE OF POSITION

5.15.1 Members shall not use their official position, official identification cards, or badges:

- For personal gain; or
- For obtaining privileges not otherwise available to them unless necessary in the performance of duty; or
- For avoiding consequences of illegal acts.

5.15.2 Members shall not lend to another person their issued uniform parts, equipment, identification cards or badges nor permit such identification cards and badges to be photographed or reproduced without the specific approval of the Colonel/Superintendent.

5.15.3 Members shall not authorize the use of their names, photographs, likenesses or official titles which identify them as members of the Massachusetts State Police in connection with testimonials or advertisements for any commodity, commercial enterprise or political purpose.

5.15.4 Members shall not become directly or indirectly involved with any arrangements, agreements, or compromises between criminals and their victims without first receiving permission from their duty assignment supervisor and consulting with the appropriate prosecuting attorney.

5.15.5 Members shall not become directly or indirectly involved with any arrangements, agreements, or compromises between criminals and any member involving restitution for lost wages, lost details or any other payment or benefit from said criminal or said criminal's agent without first receiving permission from their duty assignment supervisor and consulting with the appropriate prosecuting attorney.

5.15.6 Members shall not withhold information of any type whatsoever in order to impede or hinder an ongoing investigation, or to delay the start of such an investigation.

5.16 ENDORSEMENTS AND REFERRALS

Members shall not, in their official capacity, recommend or suggest in any manner the employment, procurement or support of any product, service, charity, or proposed law or regulation unless first authorized by the Colonel/Superintendent.

5.17 IDENTIFICATION

5.17.1 Members shall carry their issued badge(s) and photo identification card(s) on their person at all times, except when impractical or dangerous to their safety or to an investigation. They shall furnish their name, current duty assignment, and identification number to any person requesting that information when they are on- duty or while acting in an official capacity, except when the withholding of such information is necessary for the performance of Massachusetts State Police duties or is authorized by a senior supervisory member or proper authority.

5.17.2 Members who are under suspension for five or more consecutive days must turn in their issued badge(s), identification card(s), and weapon to their Division Commander before the commencement of the suspension. Members who are under suspension for thirty or more consecutive days must turn in all their issued equipment to the Supply Section before the commencement of the suspension. If any issued equipment is missing or unsuitable because of neglect or willful abuse, immediate full payment must be made to the Fiscal Section. Suspended members shall be deprived of all Massachusetts State Police powers and privileges and must not represent themselves as members of the Massachusetts State Police.

5.17.3 No member shall cause to be produced, or possess, or distribute any business card with the member's title and Massachusetts State Police information thereon, unless for an official law enforcement purpose.

5.17.4 If at a civil disturbance or other incident where the senior supervisory member has ordered helmets be worn, the helmet worn shall visibly display the member's full and accurate State Police identification number.

5.17.5 Civilian employees of the Department shall be issued an official Department photo identification card. They shall furnish their name, current assignment, and identification number to any person requesting that information when they are on duty or while acting in an official capacity, except when the withholding of such information is necessary for the performance of certain Massachusetts State Police duties or is authorized by a senior supervisory member or proper authority.

5.18 PAYMENT OF DEBTS

For the purpose of this Article a just debt or support obligation must be recognized as such by a court of competent jurisdiction before administrative action may be initiated.

5.18.1 Members shall not undertake any financial obligation which they know or should know they will be unable to meet.

5.18, continued

5.18.2 Members shall pay all just debts.

5.18.3 Members shall provide the necessary and adequate support for their immediate family and legal dependents.

5.19 POLITICAL ACTIVITY

Members are prohibited from using their official capacity to influence, interfere with, or affect the results of any election for public office. This section is not meant to interfere with the lawful activities of the collective bargaining unit representatives. In accordance with law and these Rules and Regulations, members are prohibited from:

5.19.1 Assuming active roles in the management, organization, or financial activities of partisan political clubs, campaigns, or parties;

5.19.2 Serving as officers of partisan political parties or clubs;

5.19.3 Serving in any elected public office, becoming a candidate for any public office or campaigning for any candidate seeking any public office;

5.19.4 Organizing, selling tickets to, or actively participating in a fund-raising function for a partisan political party or a partisan or non-partisan candidate;

5.19.5 Addressing a political gathering in support of, or in opposition to, a partisan candidate;

5.19.6 Engaging in prohibited partisan political activities on the Federal, state, county, or municipal level;

5.19.7 Serving as election judges or clerks or as a clerk or judge of any board or registry.

5.20 CIVIL ACTIONS

If any member shall bring a civil action, or directly or indirectly commence negotiations for settlement for damages for personal injuries incurred while in the performance of their duty, they shall immediately notify the Colonel/Superintendent, through channels and in writing, and file with the Colonel/Superintendent copies of any complaint(s) or allegation(s), and any notification of settlement(s), and also the final disposition of the action or negotiation.

5.21 RESIDENCE

Members shall reside within the territorial boundaries of the Commonwealth of Massachusetts. Any change regarding a member's domicile or mailing address, shall

5.21, continued be reported immediately, in writing, on a change of address form, to their supervisor who shall forward same to the Director of Human Resources.

5.22 TELEPHONE

Members shall, at all times, provide to their duty assignment supervisor a telephone number or numbers allowing for direct access and immediate contact.

5.23 DISSEMINATION OF INFORMATION

5.23.1 The intent of this section is to protect the members and the Massachusetts State Police against wrongful dissemination of information or its commercialization and is not intended to prevent distribution of legitimate news through proper channels.

5.23.2 Members shall treat official business of the State Police as confidential. Information regarding official business shall be disseminated only to those for whom it is intended, in accordance with established Procedures.

5.23.3 Members may remove or copy official records or reports from a State Police installation only in accordance with established Procedures.

5.23.4 Members shall not divulge the identity of any person(s) giving confidential information, except as authorized by their supervisory member or proper authority.

5.23.5 Members shall not make known any proposed action or movement of the State Police, or the contents of any Order or Directive, to persons not immediately concerned with its execution.

5.23.6 Members shall not comment for publication, nor be interviewed, nor make public speeches on police business, except by permission of the Colonel/Superintendent. Requests for talks, interviews and public speeches shall be directed to the Colonel/Superintendent through the Public Information Section.

5.23.7 No member or civilian employee shall make any type of "records inquiry" either orally, in writing, electronically, or through computer except upon official police business. The results and contents of such checks shall not be disseminated to any person or entity except in conformance with law and Massachusetts State Police Policy and Procedure, and in the course of official police business.

5.23, continued

A "records inquiry" includes obtaining information found in the records of the Registry of Motor Vehicles, and records and information available through NLETS, NCIC, CJIS, court, probation, conviction and corrections records wherever found, Massachusetts State Police records, and any other database or case records management system maintained for law enforcement or public safety purposes that is not accessible to the general public.

5.23.8 Members shall not, directly or indirectly, seek notoriety through the public media.

5.23.9 Members shall not, directly or indirectly, publicly criticize or ridicule any official action of the Massachusetts State Police or any member.

5.23.10 Members shall not directly or indirectly represent the Massachusetts State Police, nor identify themselves as a member of the Massachusetts State Police, when expressing opinions on matters outside the scope of their employment.

5.24 INTERVENTION

5.24.1 Members shall not intervene in investigations being handled by other members or by other governmental agencies unless ordered to intervene by a supervisory member or proper authority or where the situation and circumstances warrant such intervention.

5.24.2 Members shall not undertake any investigation or other official action not part of their regular duties without obtaining permission from their immediate supervisor unless the exigencies of the situation requires immediate Massachusetts State Police action. In that event, their action(s) and the reason(s) therefore shall be reported as soon as possible to their immediate duty supervisor or proper authority.

5.25 ABUSE OF PROCESS

Members shall not knowingly make untrue statements or accusations at any stage of an administrative hearing, civil proceeding or criminal proceeding, or process or application leading thereto.

5.26 USE OF EQUIPMENT

5.26.1 Members shall utilize Massachusetts State Police equipment only for its intended purpose and shall not willfully or through neglect, abuse, spoil, damage, lose, or wrongfully dispose of Massachusetts State Police equipment.

5.26, continued

5.26.2 Members shall be liable for the replacement of any Massachusetts State Police property damaged, lost or destroyed by negligence or misuse.

5.26.3 All Massachusetts State Police equipment issued to members shall be maintained in proper working order.

5.26.4 No member or civilian employee shall use Massachusetts State Police telephones, computers, postage, copiers, facsimile machines, modems, cruisers or other Massachusetts State Police supplies and equipment except for official business.

5.26.5 Members and civilian employees shall operate Massachusetts State Police vehicles in a cautious manner, and in conformance with Massachusetts State Police Policy and Procedure and applicable law.

5.26.6 Members and civilian employees shall not permit non-employees to ride in Massachusetts State Police vehicles unless due to police necessity, or where permission has been granted by the member or civilian employee's supervisor or proper authority.

5.26.7 Ride-along(s) for non-Department personnel for instructional or informational purposes shall not be permitted unless approved in advance by the member's Troop/Section/Unit Commander or designee.

5.26.8 Members shall not leave the Commonwealth of Massachusetts while on duty, or while in any Massachusetts State Police vehicle, or be in uniform while out of state, except when on official police business with permission of their supervisor or proper authority.

5.26.9 Members shall not permit any non-member to wear any part(s) of any issued Massachusetts State Police uniform assigned to them.

5.27 TRUTHFULNESS

5.27.1 Members and civilian employees shall be truthful at all times.

5.27.2 Upon the order of the Colonel/Superintendent, their designee, supervisory member, or proper authority, members and civilian employees shall truthfully answer all questions specifically directed and narrowly related to the scope of employment and operations of the Massachusetts State Police which may be asked of them. An invocation of constitutionally protected rights shall not be a violation of this Rule.

5.27.3 No member or civilian employee shall, in the course of their official duties, execute, file or publish any false written report, minutes or statements, knowing the same to be false.

5.28 OFFICIAL CORRESPONDENCE AND OFFICIAL BUSINESS

5.28.1 Members must transact all their official correspondence and official business through their Commanding Officer.

5.28.2 Massachusetts State Police stationery shall only be used for official Department business.

5.29 INTERCESSION FOR MEMBERS

5.29.1 No member shall directly or indirectly cause any person, not their duty assignment supervisor, to intercede on their behalf with supervisory members or proper authority for the purpose of seeking preferential treatment, or for transfer, re-transfer, assignment or promotion.

5.29.2 No member shall directly or indirectly cause any person, other than their duly authorized counsel where permitted, to intervene with supervisory members or proper authority relative to any official Massachusetts State Police proceeding(s) begun under these Rules and Regulations.

5.29.3 A member against whom a complaint has been made shall not attempt, directly or indirectly, by threat, persuasion, payment or promise of money, or other means to secure the withdrawal or abandonment of such complaint, or to prevent the testimony of witnesses, and shall not at any time before final judgment cause any person to intercede personally, or by letter, or in any other manner, directly or indirectly, in their behalf, with the Colonel/Superintendent or with a member of the Trial Board.

References: M.G.L. c. 22C, § 19;
MPAC: 1.2.2, 12.1.3, 22.2.7, 22.3.4, 26.1.1, 54.1.1, 82.1.7.

Promulgated by: Christopher S. Mason, Colonel/Superintendent

Department of State Police
Rules & Regulations

Effective Date:	Number:
November 10, 2021	**Article 6**

Subject:

REGULATIONS ESTABLISHING DISCIPLINARY PROCEDURES AND TEMPORARY RELIEF FROM DUTY

6.0 REGULATIONS ESTABLISHING DISCIPLINARY PROCEDURES AND TEMPORARY RELIEF FROM DUTY

6.1 TEMPORARY RELIEF FROM DUTY

6.1.1 A supervisory member shall temporarily relieve from duty and place on Administrative Leave with pay, for a period of NOT more than one workday, any member who is unfit for duty. "Unfit for Duty" may include any physical, mental or emotional condition which may, in the judgement of the supervisory member, render the member incapable of adequately performing his/her duties or causing the member to perform duties in such a way as to embarrass or discredit the Department or jeopardize the safety of himself/herself or any other person or property. A written report of the incident shall be forwarded, through channels, to the Division Commander forthwith and a copy of this report shall be made available to the relieved member. The supervisory member shall also secure any issued weapon(s), identification cards and/or other equipment in the relieved member's possession when necessary for the safety of the member or other persons.

6.1.2 Any member placed on Administrative Leave with pay in accordance with Rule 6.1.1 or Policy and Procedure UOF-03, or any member failing to meet the medical or physical fitness standards as required by law and Rules and Regulations, or any member manifesting symptoms of a physical, mental or emotional dysfunction shall, when so ordered by the Colonel, be examined or re-examined, as the case may be, by the Massachusetts State Police Surgeon to determine said member's fitness for duty. During the pendency of said examination or re-examination until otherwise ordered by the Colonel, said member shall be placed on appropriate leave or duty status. The Massachusetts State Police Surgeon shall examine said member forthwith and recommend to the Colonel in writing a duty status as follows:

6.1, continued

- Full Duty; or
- No Duty, member may use sick, vacation, personal or other accrued time as allowed by the collective bargaining agreement; or
- Temporary Modified Duty.

6.1.3 A Troop/Section/Unit Commanding Officer, through channels, may recommend to a Division Commander that a member who:

- Is the subject of a criminal investigation, is arrested or indicted or has a criminal complaint or warrant issued against him/her; or
- Is the subject of an internal investigation; or
- Engages in a strike or prohibited job action; or
- Has failed to attend and successfully complete compulsory training as mandated by the Colonel; or
- Is the subject of a court order directing said member to refrain from abusing a family or household member, or to refrain from threatening or endangering the health, safety or welfare of a family or household member.(For the purpose of this sub-part "family or household member" shall be defined in accordance with M.G.L. c. 209A §1).

Be placed on Administrative Leave with pay for a period NOT to exceed five work days. Power to issue such relief shall be vested solely in the Division Commander, with the approval of the Colonel/Superintendent. Administrative Leave shall not involve loss of pay initially; however, loss of pay relating to this period of Administrative Leave may be later imposed along with other disciplinary action. The supervisory member shall secure any issued weapon(s), identification cards and/or other equipment in the relieved member's possession when appropriate.

6.2 DUTY STATUS HEARING

6.2.1 A Division Commander, with the approval of the Colonel/Superintendent, may convene a duty status hearing relative to the member's duty status if:

- The member is the subject of a criminal investigation, is arrested or indicted or, if a criminal complaint or warrant is issued against the member; or
- The member is the subject of an internal investigation; or
- The member engages in a strike or prohibited job action; or
- The member has failed to attend and successfully complete compulsory training as mandated by the Colonel; or
- The member is the subject of a court order directing said member, to refrain from abusing a family or household member or to refrain from threatening or endangering the health, safety or welfare of a family or household member. (For the purpose of this sub-part "family or household member" shall be defined in accordance with M.G.L. c. 209A §1); or
- Exceptional circumstances exist which warrant such duty status hearing.

6.2, continued

6.2.2 The duty status hearing shall be conducted by a Board consisting of three staff and/or commissioned officers appointed by the Colonel. The Board shall expeditiously gather sufficient facts of satisfactory reliability to make a fair determination relative to the member's appropriate duty status.

6.2.3 The duty status hearing shall be under the full control of the Board, and no person, whether an official of the Massachusetts State Police or not, shall bepermitted to be present or take part without the unanimous consent of the Board.

6.2.4 The Duty Status Board shall, after a review of the facts presented, make findings and recommend to the Colonel/Superintendent whether the member should be:

- Continued on full duty;
- Placed on restricted duty;
- Suspended with pay; or
- Suspended without pay.

The Board may supplement its recommendation with a referral to the State Police Surgeon to evaluate a member’s fitness for duty, and/or a referral to the Employee Assistance Unit; provided however, said referral shall be rationally related to the incident which gave rise to the Duty Status Hearing.

6.2.5 All Duty Status recommendations shall be subject to the approval of the Colonel/Superintendent. The Colonel shall impose a Duty Status consistent with the Board's recommendation, provided however, the Colonel/Superintendent may impose a different Duty Status if facts, circumstances, evidence, aggravating or mitigating factors or any othermatters so dictate. Once approved by the Colonel, such order shall be embodied in Personnel Orders. A member's failure to strictly adhere to such order(s) shall be cause for the Duty Status Board to reconvene and reconsider the member's duty status. Failure to adhere to such order(s) may also result in independent administrative action.

6.2.6 Restricted duty shall consist of any type of limited duty approved by the Colonel/Superintendent, and shall continue in full force and effect until such time as otherwise recommended by the Duty Status Board and approved by the Colonel.

6.3 LETTER OF COUNSELING

6.3.1 After investigation a Division Commander may order that a letter of counseling be placed in a member's personnel file.

6.3.2 A letter of counseling is a formal document specifying the member's deficiency (ies).

6.3.3 If the Division Commander orders that the letter of counseling be placed in the member's personnel file, the Division Commander shall forward a copy of the letter of counseling to the member through channels. A member shall be allowed to have placed in his/her personnel file a written response or counter-statement to any letter of counseling. A letter of counseling cannot be the subject of appeal.

6.3.4 Letters of counseling shall expire one year from the date of issue. A member may request that a letter of counseling be removed from their personnel folder upon its expiration. Whenever a second or subsequent letter is filed prior to the expiration date of any preceding letter, the member may request that the letters on file be removed on the expiration date of the most recent letter.

6.3.5 This section does not limit the use of any other disciplinary procedure enumerated in these Rules and Regulations.

6.4 CHARGES AND DISPOSITION WITHOUT HEARING

Troop/Section/Unit Commanding Officers may, after investigation, recommend through channels to the Division of Standards and Training that disciplinary action be brought against members under their charge for violations of law and/or State Police Rules, Regulations, Policies, Procedures, Orders, and Directives. Such recommendations shall contain a copy of the charge form.

6.4.1 The Division of Standards and Training shall review all requests for disciplinary action and recommend to the Deputy Superintendent that charges be preferred if warranted.

6.4.2 Upon recommendation from the Lieutenant Colonel/Deputy Superintendent that a member complained against be exonerated, the Colonel/Superintendent, may, in writing, exonerate the member. Copies shall be given to the member and the appropriate Division Commander.

6.4, continued

6.4.3 When a Troop/Section/Unit Commanding Officer is notified that the Colonel/Superintendent has approved the charges and recommends corrective or disciplinary action, the Troop/Section/Unit Commanding Officer shall serve a copy of the charge form and waiver if deemed appropriate on the member against whom charges are to be preferred. The charge form shall include:

- The particular Article or Articles alleged to have been violated and the corresponding class schedule as determined in accordance with Appendix "A";
- The date or dates upon which and the place or places at which the alleged acts or omissions occurred; and
- A statement of the alleged acts or omissions.

6.4.4 One copy of the charge form shall be given to the member and the original shall be forwarded, through channels, to the Division of Standards and Training.

6.4.5 Members may waive their right to a hearing by a Trial Board and may accept such discipline as the Colonel/Superintendent may offer and prescribe, including discharge.

6.4.6 In the event a member does not elect to waive the right to a Trial Board, the Colonel/Superintendent shall issue an order, in writing, for disciplinaryaction in accordance with Rule 6.7. Copies shall be given to the member and the appropriate Division Commander.

6.5 HEARING ON CHARGES

6.5.1 A member who has served for one year or more and has been formally charged in accordance with Departmental Rules and Regulations shall be tried by a State Police Trial Board appointed by the Colonel/Superintendent. Alternatively, the member may request that s/he be tried by a Board consisting of the Colonel. Any request for a hearing before the Colonel shall be made in writing and subject to the Colonel's approval.

6.6 DEPARTMENTAL PROSECUTOR

6.6.1 The Lieutenant Colonel/Deputy Superintendent shall appoint a Commissioned Officer as the Departmental Prosecutor. The Department Prosecutor shall present evidence, call witnesses, and cross-examine witnesses on behalf of the Department.

6.7 TRIAL BOARDS

6.7.1 A State Police Trial Board shall hear cases regarding violations of Rules, Regulations, Policies, Procedures, Orders, or Directives. A Trial Board hearing shall be a formal administrative proceeding

6.7.2 A Trial Board shall consist of three staff and/or commissioned officers appointed by the Colonel/Superintendent. The Board shall be presided over by a President, as designated by the Colonel/Superintendent. The President shall designate a member of the board as Secretary.

6.7.3 No member of a Trial Board shall sit in a hearing in which a member of his/her own Troop/Section/Unit is either a complainant or defendant; nor, shall s/he sit in on any other case in which his/her personal or official relations to either party or to counsel might properly raise a question of impartiality. Said member shall be excused and replaced by an alternate.

6.7.4 The charged member, prior to the hearing date, may request a continuance. Continuances may be granted by the Colonel/Superintendent. No continuance shall be granted within seventy-two hours of the Trial Board Hearing unless extenuating circumstances warrant the granting of such continuance. If criminal charges are pending against the charged member, the hearing may be postponed until after the criminal disposition.

6.7.5 The hearing shall be under the full control of the Board, and no person, whether an official of the Department or not, shall be permitted to bepresent or take part without the unanimous consent of the Board.

6.7.6 The charged member is entitled to be represented by counsel, but counsel shall not be provided by the Massachusetts State Police. All proceedings shall be recorded. The charged member shall have the right to present evidence, to call witnesses on his/her behalf, and to cross-examine witnesses against him/her. Witnesses shall testify under oath or affirmation. The Trial Board is not bound to follow strict rules of evidence.

6.7.7 Upon the completion of the testimony presented by the prosecution and defense, the Board shall accept evidence from the Department prosecutor of prior offenses/disciplinary history. Any such records or evidence submitted shall be used only after the charges have been adjudicated by the Trial Board and for the sole purpose of recommending discipline under Rule 6.9. Should the member wish to

6.7, continued

address the Board on the issue of any such priordiscipline, the Board shall hear any such additional arguments.

6.7.8 The Trial Board, by a majority vote and in writing shall summarize the evidence, and make findings of fact. The Trial Board shall enter a determination of "Guilty" or "Not Guilty" for each charge/specification. In the event that the Trial Board finds guilt by a preponderance of the evidence on one or more of the charges, the Trial Board shall consider the evidence presented by the Department prosecutor pertaining to the accused member's prior offenses/disciplinary history, and shall make recommendations for administrative action in accordance with Rule 6.9. The Board shall forward said findings to the Lieutenant Colonel/Deputy Superintendent. Should the Board recommend increased discipline under the Discipline Guidelines, the Trial Board should note the same in its recommendation, referring to specificprior offenses. In the event the Trial Board finds the member not guilty, such finding shall be final and conclusive, except as otherwise provided by law.

6.8 DEPUTY SUPERINTENDENT'S ACTION

6.8.1 Upon receipt of the trial record, the Lieutenant Colonel/Deputy Superintendent shall review all summaries, findings, reports, and recommendations received.

6.8.2 If the Trial Board's decision is adverse to the accused member, the Lieutenant Colonel/Deputy Superintendent shall forward a copy of the proposed decision to the member provided, however, a request was made to file objections with the Colonel seven (7) days prior to the hearing date. Absent such a written request, the provisions of this section shall be deemed waived. The accused member shall have seven (7) days from receipt of the proposed decision to file written objections to the Colonel.

6.8.3 After receipt and review of written objections as provided in Rule 6.8.2, the Lieutenant Colonel/Deputy Superintendent shall make, in writing to the Colonel/Superintendent, any recommendations as may be determined by thefacts of the case and forward the Trial Board decision, written objections and recommendations to the Colonel/Superintendent.

6.9 JUDGEMENTS AND DISCIPLINE

6.9.1 The Trial Board shall recommend discipline in accordance with Rules 6.9.2, 6.9.3 and 6.9.4.

6.9.2 Recommendations for discharge, suspension, loss of accrued vacation/personal/holiday time, and reprimands (s) in Personnel Orders shall be made in accordance with the Appendix "A" Guidelines. All disciplinary recommendations made by the Trial Board shall fall within the parameters of the Appendix "A" Guidelines; provided however, the Trial Board may supplement its recommendation with a petition to theColonel/Superintendent requesting that s/he consider a departure from said guidelines. In the event the Trail Board elects to file a supplemental petition, such petition shall state in writing facts, circumstances, evidence, aggravating or mitigating factors, or any other matters that may warrant such consideration.

6.9.3 Notwithstanding Rule 6.9.2, the Trial Board may recommend other additional discipline as it deems appropriate including, but not limited to alternative duty (6.9.8), transfer, limiting paid details or overtime, and reduction in one or more titles of rank.

6.9.4 The Trial Board shall recommend discipline for each offense for which the member is found guilty; provided however in the event of multiple offenses the Board shall further recommend whether such discipline should be imposed consecutively or concurrently. All such recommendations shall be forwarded to the Lt. Colonel/Deputy Superintendent in accordance with Rule 6.8.

6.9.5 All judgments of guilt entered or, discipline recommended by the Trial Board or recommendations made in accordance with Rule 6.8.2, shall be subject to the approval of the Colonel/Superintendent and, when so approved, shall be final and conclusive except as otherwise provided bylaw. Disciplinary action imposed by the Colonel/Superintendent, shall be in writing, duly entered upon the record and embodied in Personnel Orders and a copy thereof placed in the member's personnel file.

6.9.6 In the event the Trial Board finds a member not guilty, such finding shall befinal, conclusive and binding on all parties. In the event the Trial Board finds a member guilty and the Colonel/Superintendent finds material error in the procedure, judgment, or disciplinary recommendation of a Trial Board, the Colonel may order a new Trial Board, or direct that one or more charges against the accused be

6.9, continued

dismissed or impose discipline in accordance with Rule 6.9.5 and 6.9.7.

6.9.7 The Colonel/Superintendent may impose discipline that departs from the Guidelines if facts, circumstances, evidence, aggravating or mitigating factors, or any other matters so dictate. In the event the Colonel/ Superintendent departs from the Guidelines, the Colonel/Superintendent shall put forth in writing his/her justification for such departure.

6.9.8 If alternative duties are recommended by the Trial Board and approved by the Colonel/Superintendent, they shall be performed under the direction of the member's Troop/Section/Unit Commanding Officer. When the disciplinary action has been completed, the Troop/Section/Unit Commanding Officer shall so certify in writing to the Lieutenant Colonel/Deputy Superintendent.

Promulgated by: Christopher S. Mason, Colonel/Superintendent

Department of State Police
Rules & Regulations

Effective Date:	Number:
November 10, 2021	**Article 7**

Subject:

REGULATIONS ESTABLISHING ENLISTMENT, DISCHARGE AND RESIGNATION

7.0 REGULATIONS ESTABLISHING ENLISTMENT, DISCHARGE AND RESIGNATION

7.1 ENLISTMENT

7.1.1 No trainee or member shall procure his appointment or enlistment or continue in enlistment by means of any willful misrepresentation or misstatement.

7.1.2 Enlistment within the Massachusetts State Police is dictated by the terms of M.G.L. c. 22C §10.

7.1.3 During the first twelve months following a member's initial enlistment members shall be retained on a probationary status. During the probationary period, the Colonel/Superintendent may, as allowed by law,discharge any member.

7.1.4 As condition precedent to a member's continued enlistment, said member shall undergo an in-service medical and physical fitness examination and shall meet such in-service medical and physical fitness standards as provided by law and as prescribed by the Colonel/Superintendent.

7.2 DISCHARGE

7.2.1 An HONORABLE discharge may be given to members of the Massachusetts State Police:

- Upon retirement in good standing; or
- Upon separation for illness or injury incurred through no fault of the member, in the actual performance of duty, and where the member's record of service merits such discharge.

7.2, continued

7.2.2 An ORDINARY discharge may be given under honorable conditions to members of the Massachusetts State Police:

- Resigning at their own request.

7.2.3 A GENERAL discharge may be given to members of the Massachusetts State Police not complying with conditions applicable to an honorable or ordinary discharge. A GENERAL discharge shall mean the complete and final severance from any duty with the Massachusetts State Police.

7.2.4 A DISHONORABLE discharge may be given to any member of the Department who is;

- Discharged following a Trial Board, or is discharged after having waived their right to a Trial Board;
- Separated from service while a Trial Board is pending or before completion of the full and complete discipline imposed following aTrial Board;
- Separated from service after being charged with or convicted of a criminal offense; or
- Separated from service while the subject of an administrative orcriminal investigation.

7.2.5 A member of the Department who has been dismissed from the State Police after a hearing before a Trial Board, or who resigned while charges were pending against that member, shall not be reinstated by the Colonel/ Superintendent. Any member granted a GENERAL or DISHONORABLE discharge shall not be reinstated by the Colonel/Superintendent.

7.3 RESIGNATION

7.3.1 Members of the Massachusetts State Police who resign voluntarily shall submit their resignations to the appropriate Division Commander, in writing, at least one month in advance of the anticipated date of separation. The Division Commander shall notify the Personnel Section forthwith.

7.3.2 A member shall remain subject to State Police Rules, Regulations, Policies, Procedures, Orders and Directives until their resignation or retirement is effective.

7.3.3 All resignation requests shall be investigated by the member's Troop/Section/Unit Commanding Officer. All Troop/Section/Unit Commanding Officers shall state in their endorsement on all resignations whether or not the member should be recommended for future reinstatement. When a member resigns after charges have been preferred or while charges are pending, the Troop/Section/Unit Commanding Officer shall state in their recommendations what the specific charges are and the reason for same

Promulgated by: Christopher S. Mason,Colonel/Superintendent

Department of State Police
Rules & Regulations

Effective Date:	Number:
November 10, 2021	**Article 8**
Subject:	
REGULATIONS ESTABLISHING THE BOARD ON CLAIMS	

8.0 REGULATIONS ESTABLISHING THE BOARD ON CLAIMS

8.1 Under the authority granted by M.G.L. c. 22C, there is established within the MassachusettsState Police a Board on Claims for physical injuries.

8.1.1 The Board on Claims shall hear cases of claims relating to injuries incurred by any member or trainee (while in training) actually performing police services or while such member or trainee is traveling to and from a duty assignment.

8.1.2 The Board on Claims shall be appointed by the Lieutenant Colonel/Deputy Superintendent with the approval of the Colonel/Superintendent and shall consistof three members as follows:

- Two staff and/or commissioned officers of the Department; and
- The State Police Surgeon.

8.1.3 One staff or commissioned officer shall be designated by the Lieutenant Colonel/ Deputy Superintendent as the President.

8.1.4 One staff or commissioned officer shall be designated by the President of the Board on Claims as the Secretary.

8.1.5 The members of the Board on Claims shall review all appropriate and available information relating to any claim of physical injury alleged by a member or traineeto have occurred in the line of duty.

8.1.6 The Board on Claims shall be conducted in an informal manner and may proceedin any manner as it deems fair and appropriate. The Board on Claims may obtain any investigative reports, documents, and bills of debit that may relate to the claim.

8.1.7 The Board on Claims may require an employee to undergo additional evaluation asappropriate.

8.1.8 At the conclusion of a Board on Claims hearing, the panel, in writing, shall summarize the claim and make findings.

8.1.9 The President of the Board of Claims through channels and in writing, shall notify the member or trainee of any action taken.

8.1.10 The Department shall be reimbursed forthwith by any member or trainee for the sums as have been paid to the injured member or trainee, or on his/her behalf, as injury related costs and wages, provided that the injured member has been reimbursed by the person(s) or organization(s) responsible for the accident or injury.

Promulgated by: Christopher S. Mason, Colonel/Superintendent

Department of State Police
Rules & Regulations

Effective Date:	Number:
November 10, 2021	**Article 9**
Subject: **REGULATIONS ESTABLISHING EXAMINATION APPEAL**	

9.0 REGULATIONS ESTABLISHING EXAMINATION APPEAL

9.1 The Colonel/Superintendent or his/her designee shall administer the appeal process for recruit entrance exams and promotional exams as established by Massachusetts State Police Rules, Regulations, Policy, Procedure, Order, or Directive and applicable law.

9.2 The appeal process for recruit candidates shall include the following elements:

9.2.1 The marking of an applicant's answers to the questions on such entrance examination.

9.2.2 A finding by the Colonel/Superintendent that an applicant does not meet the entrance requirements for such examination or that such applicant does not meet age requirements.

9.2.3 The suitability of a question to test the fitness of such member to performthe primary and dominant duties of the position for which the examination was held.

9.3 An Appeals Board consisting of three staff and/or commissioned officers appointed by the Colonel shall review all promotional examination appeals and make written recommendations to the Colonel.

9.4 Appeals regarding promotional examinations shall be limited to the following:

9.4.1 A finding by the Colonel that a member does not meet the requirementsfor such examination.

9.4.2 The marking of a member's answers to the questions on such promotional exam.

9.4, continued

9.4.3 The suitability of a question to test the fitness of such members to performthe primary and dominant duties of the rank for which the examination was held.

9.5 In determining appeals filed pursuant to Rule 9.4.1, the Board shall utilize Departmental records to determine whether a member meets the requirements set forth in M.G.L. c. 22C.

9.6 In determining appeals filed pursuant to Rule 9.4.2 the Board shall consider the following:

- Does the question contain any material typographical or syntax errors?;
- Is the keyed answer correct according to the master answer sheet?;
- Is the intended key the best of the available choices?; and
- Was the marking of the member's answers to the questions correctly recorded?

9.7 In determining appeals filed pursuant to Rule 9.4.3, the Board shall determine, (1) whether the question was drawn from recommended source material and, (2) whether the question and the source material reasonably test the fitness of a member to perform the primary and dominant duties of the rank for which the examination was administered. When determining whether the question and the source material reasonably test the fitness of a member to perform the primary and dominant duties of the rank for which the examination was administered, the Board shall observe, and be guided by, the current job classification specifications for such rank.

9.8 The Colonel shall establish in Departmental Orders the time and manner when appeals shall be filed. All appeals shall be in writing.

Promulgated by: Christopher S. Mason, Colonel/Superintendent

Department of State Police
Rules & Regulations

Effective Date:	Number:
November 10, 2021	**Article 10**

Subject:

REGULATIONS ESTABLISHING RECRUIT MINIMUM ENTRANCE REQUIREMENTS

10.0 REGULATIONS ESTABLISHING RECRUIT MINIMUM ENTRANCE REQUIREMENTS

10.1 Candidates considered to appointment must:

10.1.1 Satisfy all statutory requirements for appointment to the Massachusetts State Police Academy;

10.1.2 Demonstrate themselves to be of good moral character, have a sound work ethic, are capable of decision making consistent with the Oath of Office, and are otherwise suitable for appointment to the Massachusetts State Police Academy;

10.1.3 Be qualified and deemed suitable by the Colonel/Superintendent to possess a valid Massachusetts Firearms License upon appointment to the Massachusetts State Police Academy;

10.1.4 Possess a high school diploma, a General Educational Development (GED) certificate, or a High School Equivalency (HiSET) certificate upon appointment to the Massachusetts State Police Academy;

10.1.5 Satisfy the Department's physical fitness standards for initial appointments, as promulgated and amended;

10.1.6 Satisfy the Department's medical and psychological standards for initial appointment, as promulgated and amended;

10.1.7 Be a United States Citizen upon appointment to the Massachusetts State Police Academy;

10.1.8 Possess a valid Massachusetts Driver's License upon appointment to the Massachusetts State Police Academy;

10.1.9 Be a Massachusetts resident upon appointment to the Massachusetts State PoliceAcademy;

10.1, continued

10.1.10 Be in compliance with Department of State Police General Order GEN-01A Tattoos and Body Modifications; and

10.1.11 Meet all other eligibility and entrance requirements duly established by statute, rule, regulation, policy, procedure, directive, and/or order of the Commonwealth of Massachusetts Department of State Police, including but not limited to Classification Specification promulgated for the position of a Massachusetts State Police Trooper, as amended.

10.2 Candidates satisfying all of the minimum entrance requirements shall, in accordance with Massachusetts General Laws c.22C §11, be considered for appointment to the Massachusetts State Police Academy. However, satisfaction of the minimum requirements by a candidate shall not guarantee appointment to the Massachusetts State Police.

Promulgated by: Christopher S. Mason, Colonel/Superintendent

CRUISER	YEAR	MAKE	MODEL	TYPE	TPR	nstalled	In PersonTraining	HOST NAME

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



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

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

Processor S/N	MSP Inv. #	IP	Need to do
G.L. c. 4.sec. 7. cl.26(f)(investigative), G.L. c. 4.sec. 7.cl.26 (n)(security)			

Reported Porblems	Annual update /cal
G.L. c. 4.sec. 7. cl.26(f)(investigative), G.L. c. 4.sec. 7.cl.26 (n)(security)	[redacted]

2386
DOUGLAS R. HOFFER
STATE AUDITOR

STATE OF VERMONT
OFFICE OF THE STATE AUDITOR

To: Representative Maxine Grad, Chair of the House Committee on Judiciary
Senator Dick Sears Jr., Chair of the Senate Committee on Judiciary
Representative Patrick Brennan, Chair of the House Committee on Transportation
Senator Dick Mazza, Chair of the Senate Committee on Transportation
Date: September 27, 2018
Re: Statutory Compliance of Automated License Plate Recognition Systems in Vermont
Cc: Thomas Anderson, Commissioner of the Department of Public Safety

Introduction

Automated License Plate Recognition system (ALPR) units are mounted on police vehicles, traffic lights, and street signs. The units automatically record images of license plates and enter the license plate numbers as well as GPS coordinates and other information into a database. The database can later be searched, and the information retrieved can help law enforcement locate where vehicles were at a specific time and place. Many states regulate the use of ALPR systems, mostly through access and data retention policies.[1] Such policies are generally driven by privacy concerns and vary widely. For example, New Hampshire law requires that ALPR records be deleted within three minutes of their capture, while Colorado allows records to be retained for three years.[2]

Act No. 175 of 2018 requires the State Auditor's Office (SAO) to examine requests for ALPR historical data that resulted in a release of information by the Vermont Intelligence Center (VIC) to the requester from July 1, 2016 through June 30, 2018. The objective of the examination is to determine whether requests and releases of historical ALPR data complied with the requirements of 23 V.S.A. § 1607.[3]

Highlights

- SAO reviewed all sixty-four requests for historical ALPR data that resulted in the release of information reviewed during the period specified in Act 175. Fifty-seven appeared to comply with 23 V.S.A. § 1607, while seven did not.
- Six of seven releases of information that did not comply with statute provided historical data older than six months, which requires the requester to obtain a warrant or there must be pending criminal charges.
- One request did not provide specific and articulable facts, as required by law.

1 "Automated License Plate Readers: State Statutes Regulating Their Use," National Conference of State Legislatures, available here.

2 "Automated License Plate Readers: State Statutes Regulating Their Use," National Conference of State Legislatures, available here.

3 Act 175 of 2018

Statute and VIC

Law enforcement agencies can request ALPR historical data to aid their investigations. Historical data "means any data collected by an ALPR system and stored on the statewide ALPR server…" operated by the VIC.[4] 23 V.S.A. § 1607 states that to be approved, "the request must provide specific and articulable facts showing that there are reasonable grounds to believe that the data are relevant and material to an ongoing criminal, missing person, or commercial motor vehicle investigation or enforcement action." The request must include the name of the requester, the requester's law enforcement agency, and the law enforcement agency's Originating Agency Identification (ORI) number. Furthermore, as noted above, statute specifies that historical data older than six months may only be released if it is related to pending criminal charges or a warrant has been issued.[5]

According to the VIC, analysts rely on the information on the ALPR Request Form when determining whether to approve a request for historical data. Specifically, they ensure that there is a case number, the approval of the supervisor of the requesting law enforcement officer, and that the written request does not appear to be "fishing" for information. The VIC notes that "specific and articulable facts" and "reasonable grounds" are subjective standards, and each request is examined with the context provided on the form. Furthermore, VIC specified that it does not determine whether information is necessary for an investigation and does not verify the information provided by the requester.[6] [7]

Compliance with Statute

From July 1, 2016 to June 30, 2018, VIC approved 339 requests for a search of historical data made by local, state and federal law enforcement agencies, 64 of which resulted in the release of information to the requester.[8] As specified by Act 175, SAO examined the 64 that resulted in the release of historical data. SAO did not assess the accuracy of the information on the ALPR Request Forms provided by the VIC. For example, we did not verify statements made by law enforcement officers; our analysis assumes that professional law enforcement provided accurate information on the ALPR Request Forms. Further, we did not examine requests that were approved but did not result in the release of historical information.[9]

4 23 V.S.A. § 1607

5 23 V.S.A. § 1607

6 Statute does not require that VIC determine whether information provided on the form is relevant to an investigation and does not require that the VIC verify information provided by the requester. SAO includes this information to provide relevant context about how VIC carries out its duties.

7 August 2018 discussion with VIC.

8 Specifically, the VIC approved the request for information based on information provided by a law enforcement agency with an ALPR Request Form, and found information in the ALPR database relevant to the ALPR request. In many cases, requests are approved but no relevant information is found in the database, and as a result no information is released to the requesting law enforcement agency.

9 VIC only releases historical data after approving the request and if relevant data is found in the database.

132 State Street ♦ Montpelier, Vermont 05633-5101
802.828.2281 ♦ Toll-Free in VT only: 877.290.1400 ♦ Fax: 802.828.5599
aud.auditor@vermont.gov♦ www.auditor.vermont.gov

We examined ALPR Request Forms for each element that is required by statute. Most met the requirements in 23 V.S.A. § 1607. However, requests for historical data varied widely in the level of detail provided. Some offered a narrative explaining why historical data would be useful to an investigation, while others provided very little information. For example, one case provided details about a crime that occurred at a certain location, a witness to that crime, the type of vehicle the witness described, and how the ALPR historical data might be useful to the active investigation. In contrast, another request merely stated that the information was to track a certain vehicle of "drug traffickers from [city name]." Appendix A includes further examples of the variation in level of detail provided by law enforcement on ALPR Request Forms.

Seven requests and subsequent information releases did not comply with statute. Six requests resulted in the release of historical data older than six months, which statute specifies requires a warrant or pending criminal charges.[10] The releases of historical data older than six months occurred in 2016 and 2017, and data released were up to eighteen months old. The ALPR Request Forms did not include or reference a warrant or pending criminal charges.

VIC agreed that they were not in compliance with the statute, which went into effect on July 1, 2016, and they stated that they were not in compliance until "mid-2017." Subsequently, the VIC retrained their analysts and changed their request review procedures to include a review of each ALPR by a second analyst.[11]

Of the seven requests that resulted in the release of historical data but did not comply with statute, one lacked specific and articulable facts. The request, made by a local police department, stated that the request was for a "Drug investigation," and identified a vehicle but provided no other details. This does not meet a standard of "specific and articulable facts" that would provide reasonable grounds to believe that the data are relevant to an ongoing investigation because the request simply states that there is a drug investigation but does not explain why the data would be relevant to the investigation itself.

Conclusion

Of 64 releases of historical data reviewed by SAO, 57 appeared to comply with 23 V.S.A. § 1607, while seven did not. Six of seven provided information older than six months without a warrant or a pending criminal charge, while one request provided no "specific and articulable" facts. While 11 percent of reviewed cases did not comply with statute, 89 percent met the statutory requirements.

The legislature could take a variety of actions to safeguard ALPR historical data. As mentioned, statute requires that the requester "provide specific and articulable facts showing that there are reasonable grounds to believe that the data are relevant and material" to ongoing investigations. The legislature

10 Act 169 of 2015 amended 23 V.S.A. § 1607 to specify that no historical data older than 6 months be released without a search warrant or pending criminal charges. The relevant section of Act 169 went into effect on July 1, 2016. All reviewed requests came at least three months after the provisions in Act 169 went into effect.

11 September 5, 2018 email with VIC.

132 State Street ♦ Montpelier, Vermont 05633-5101
802.828.2281 ♦ Toll-Free in VT only: 877.290.1400 ♦ Fax: 802.828.5599
aud.auditor@vermont.gov♦ www.auditor.vermont.gov

could further specify how “specific and articulable facts” and “reasonable grounds” are defined. Such a definition might be developed in consultation with local and state law enforcement agencies to create a workable definition for law enforcement balanced against privacy concerns.

Furthermore, the legislature could require historical data requesters to attest that the information they have provided on an ALPR Request Form is accurate and truthful to the best of their knowledge. Finally, the legislature could require the VIC to annually conduct an internal audit of their ALPR system process to ensure statutory compliance and improve the procedure.

We appreciate the assistance of VIC and DPS staff during this review.

Appendix A: ALPR Request Form Details Examples

Requests for historical data varied widely in the level of detail provided. Some offered a narrative explaining why historical data would be useful to an investigation, while others provided very little information. Here we have provided six redacted examples of the information provided by law enforcement agencies on ALPR Request Forms. In addition to the information provided below, ALPR Request Forms often include specific vehicle information.

1. “Investigation into multiple ATM robberies spanning multiple counties in the State of Vermont. The suspect has been associated with VT registration: [license plate, make of vehicle] The first ATM robbery occurred [date] and the latest was on [date].”

2. “Vehicle reported to be a stolen rental car. Possibly involved in frequent trips between [City] and VT.”

3. “Suspects vehicle in car theft.”

4. “The following vehicle may be involved in drug trafficking from [state] to the Vermont. The intended suspect to the investigation is [name, date of birth] and the vehicle was rented from [car rental company]. The projected search of the system of VT and [state] is to verify information given from a cooperating subject that he is traveling to and from [state] frequently to traffic heroin and cocaine back to VT in this vehicle.”

5. “Historical Query on individual’s vehicle to see if it has been seen in Vermont over the last year or so. Individual is associated with known marijuana smugglers and may be participating in the movement of illicit drugs.”

6. “[Name] is suspected of selling heroin in the [town 1] and [town 2] area. He is also possibly linked to a fatal overdose in [town 2].”

132 State Street ♦ Montpelier, Vermont 05633-5101
802.828.2281 ♦ Toll-Free in VT only: 877.290.1400 ♦ Fax: 802.828.5599
aud.auditor@vermont.gov♦ www.auditor.vermont.gov

Massachusetts Department of State Police
Automated License Plate Recognition (ALPR) System
Memorandum of Understanding and Agreement

THIS AGREEMENT, made and entered into this 3rd day of May, 2023 by and between the Department of State Police, hereinafter referred to as "Department," and the Chicopee 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.

Colonel John E. Mawn, Jr. Massachusetts State Police	Representative: Deputy Chief Eric Watson Agency:
Date	5/3/23 Date

Department of State Police
DIVISION COMMANDER'S ORDER

Issue Date	**Number**
September 13, 2023	**2023-DHS-013**
Subject: **ALPR Data Retention & Access**	

The Division of Homeland Security and Preparedness is responsible for the administration of the Department's Automatic License Plate Recognition (ALPR) system. The availability and use of ALPR technology significantly enhances public safety by augmenting the operational and investigative effectiveness of law enforcement agencies.

The use of ALPR technology is governed by General Order TRF-11 "Automatic License Plate Recognition". In addition, the use of ALPR systems shall be subject to the guidelines set forth in this Order unless superseded by General Order TRF-11.

Pursuant to General Order TRF-11, the retention of ALPR data collected by the Department shall be determined by the Department of Criminal Justice Information Services (DCJIS) policy. Furthermore, ALPR systems operated by the Department shall be configured to restrict data visibility for a maximum duration of sixty (60) days from the date of the initial request.

Users requesting to access records beyond sixty (60) days, shall contact the Commonwealth Watch Center, the ALPR Administrator, or other administrator authorized by the Division Commander of Homeland Security and Preparedness. The request will be reviewed on a case-by-case basis. In the absence of exigent circumstances, the user may be required to revise their request, consult with a District Attorney's Office of jurisdiction, or to submit legal process to obtain the requested records.

_____

Mark D. Cyr
Lieutenant Colonel
Division of Homeland Security and Preparedness

Location:
MOTOR VEHICLES REGISTRATION;
Scope:
Other States laws/regulations; Program Description;

OLR RESEARCH REPORT

November 6, 2012 2012-R-0482

AUTOMATIC LICENSE PLATE RECOGNITION SYSTEMS

By: Duke Chen, Legislative Analyst II

You asked for information on automatic license plate recognition (ALPR) systems, specifically if (1) Connecticut has had any proposals banning their use, (2) any states ban or limit them, and (3) any countries have banned them.

SUMMARY

Generally, ALPR systems automatically capture an image of a vehicle's license plate and compare the plate with one or more databases of vehicles ALPR systems can be deployed in police cars or mounted at an intersection and be used to find stolen or uninsured vehicles. But there are concerns about inaccurate data and privacy when it comes to ALPR use.

We were unable to find any proposed legislation in Connecticut that would ban ALPR systems, but there has been at least one proposal limiting the data retention period

At least two states, New Hampshire and Maine, have laws limiting ALPR technology. New Hampshire has, with certain exceptions, a general ban. Maine only allows certain public safety agencies to use the technology. These agencies can retain the information for up to 21 days In addition to these state laws, New Jersey, through an Attorney General Directive, provides a guideline for its law enforcement agencies, which includes limiting their data retention to five years.

We were unable to find any countries that completely ban ALPR systems.

ALPR

Law enforcement agencies throughout the nation are increasingly using ALPR technologies to enhance their enforcement and investigative capabilities. They use the technology to expand their collection of relevant data and expedite the time consuming process of license plate comparisons

The database expansion combined with the rapid results of the scans allows law enforcement to find uninsured or stolen cars more quickly and efficiently.

How ALPR Works

ALPR systems (1) automatically capture an image of a vehicle's license plate, (2) convert the image into alphanumeric characters, and (3) compare the number with the database of interest. All of this occurs in seconds, which allows law enforcement to quickly determine if the car is stolen, uninsured, or wanted for other law enforcement reasons.

Concerns About the Technology

There are concerns about inaccurate data and privacy with the use of ALPR technology If inaccurate data is added to the databases, there could be false hits due to the faulty data.

There are also privacy concerns about law enforcement agencies recording the location of a person's car. In addition to the privacy concerns arising from the scans themselves, there are concerns about how long the data is retained

CONNECTICUT

We were unable to find any proposed legislation that would have banned ALPR systems. But, there has been at least one proposal to limit the data retention of ALPR technology.

In 2012, the public safety committee held a public hearing on HB 5391 The bill would have required law enforcement agencies that use ALPR systems to expunge the data from the system within 14 days after collection, unless the data was relevant and material to an ongoing criminal investigation or prosecution.

After the public hearing, the Public Safety Committee referred the bill to the Insurance Committee. The Insurance Committee approved a substitute bill by a 15-4 vote and referred it to the House floor, where no further action was taken.

OTHER STATES

New Hampshire

New Hampshire generally bans surveillance on highways, including the use of ALPR systems (N.H. Rev. Stat. Ann. § 236:130). This prohibition includes the state as well as private citizens.

The New Hampshire law does allow for certain exceptions, including certain investigatory, traffic, and security purposes.

Any person violating these provisions is guilty of a violation, which is punishable by up to a $1,000 fine. Other entities violating these provisions are guilty of a misdemeanor, which is punishable by up to a $1,200 fine

Maine

Maine only allows its departments of Transportation and Public Safety and law enforcement agencies to use ALPR systems for certain public safety purposes (Me. Rev. Stat. Ann. 29-A, § 2117 A)

2398
The law provides that the data that is collected is confidential and can only to be used by law enforcement in carrying out its duties. Furthermore, the data collected or retained may not be stored for more than 21 days.

A violator is guilty of a class E crime, which is punishable by up to six months imprisonment and a $1,000 fine

New Jersey

Through a New Jersey Attorney General Directive, law enforcement in the state must adhere to certain guidelines (http://www.state.nj.us/oag/dcj/agguide/directives/Dir-2010-5-LicensePlateReadersl_120310_pdf)

These guidelines include limitations on when ALPR systems may be deployed, used, and who is qualified for such use. In addition, each department that uses an ALPR system must keep a record of when and where it was deployed, if it was mobile or fixed, and if any data was transferred or stored

The guidelines also require all records of ALPR activity to be maintained for five years and be readily accessible for audit. After the five years, the data must be purged from the system.

DC ro

Massachusetts Department of State Police
Automated License Plate Recognition (ALPR) System
Memorandum of Understanding and Agreement

THIS AGREEMENT, made and entered into this 30 day of MAY, 2023 by and between the Department of State Police, hereinafter referred to as "Department," and the Braintree 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.

Colonel John E. Mawn, Jr.
Massachusetts State Police

Date

Representative: MARK DuBois
Agency: Braintree Police Dept

05/30/23
Date

2404



Chorus Intelligence Suite

Discover • Link • Solve

Chorus

Discover • Link • Solve



One intelligence platform to empower your entire organization to tackle the biggest crime types, including:

- Gang and organized crime
- Violent crime
- Mass gatherings/civil unrest
- School safety issues
- Gun crime
- Human trafficking
- Narcotics

The current state of Policing

What we know

- Crime detection rates are low and have deteriorated.
- Online crime is now by far the most prevalent crime type.
- There are increased demands to tackle organized crime via collaboration and data sharing.
- Law enforcement is faced with resourcing issues and cannot meet demand.
- Funding issues now require law enforcement to do more with less.



What we're doing about it

We have developed the Chorus Intelligence Suite (CIS) to support analysts, investigators and front-line officers in conducting end-to-end digital investigations via **one platform, one dashboard and one login**. Intuitive tools can be used by all to combine analytical data with OSINT and internal data, to easily identify patterns, spot connections and open further lines of inquiry.

Increase detection rates

Combine analytical data with OSINT and internal data to never miss a connection

Empower multiple roles

Enable investigators and front-line officers to easily get answers from data

Save money

Connect disparate systems into one platform to find the data that you need

Collaborate & share

Collaborate and share cases with colleagues, partners and external organizations

Optimize efficiency

Store, index, search, analyze and report on ALL data in one place

Safe and secure

A Software as a Service (SaaS), platform, which protects anonymity

The Chorus Intelligence Suite

Be empowered at every stage of a digital investigation to realize the full potential of your data.

Case management & sharing — Page 5

Store and share all your investigative data in a central and fully secure digital hub.

Federated search & enrichment — Page 6-7

Query any entity and search across your internal files, consented data and over 200+ social media platforms to fast track the attribution process.

Secure open-source capture — Page 8

Capture any webpage, image or video in a single click from a secure and anonymous environment.

Internal data integration — Page 9

Securely upload any internal or unstructured, disparate legacy files into the CIS to centralize your investigative data.

Data cleansing & analysis — Page 10-11

Drag and drop any digital data into the CIS to be automatically cleansed and formatted, saving 97% of your time.

Evidential reporting — Page 12

Overlay internal, external and consented data to interrogate in multiple ways and generate courtroom-ready reports.

Case Management & Sharing

Search an entity from an internal file against your operational and historical files to see if it has previously appeared.

Key capabilities include:

- **Create and collaborate** - Securely access the CIS from any browser to quickly and easily create, view and collaborate on cases. Any data that is uploaded or captured within the CIS can be indexed and searched.
- **Bulk search data for cross-case analysis** - Search across your operational and historical files.
- **Apply audit and access controls -** Choose who can view and edit cases, depending on their security level. Maintain audit logs to document when any searches, web captures and activities are performed, by whom and when.
- **Redact and report** - The CIS recognizes keywords, phone numbers or names from captured digital evidence, which can be automatically or manually redacted before generating a report.

CJIS Compliant



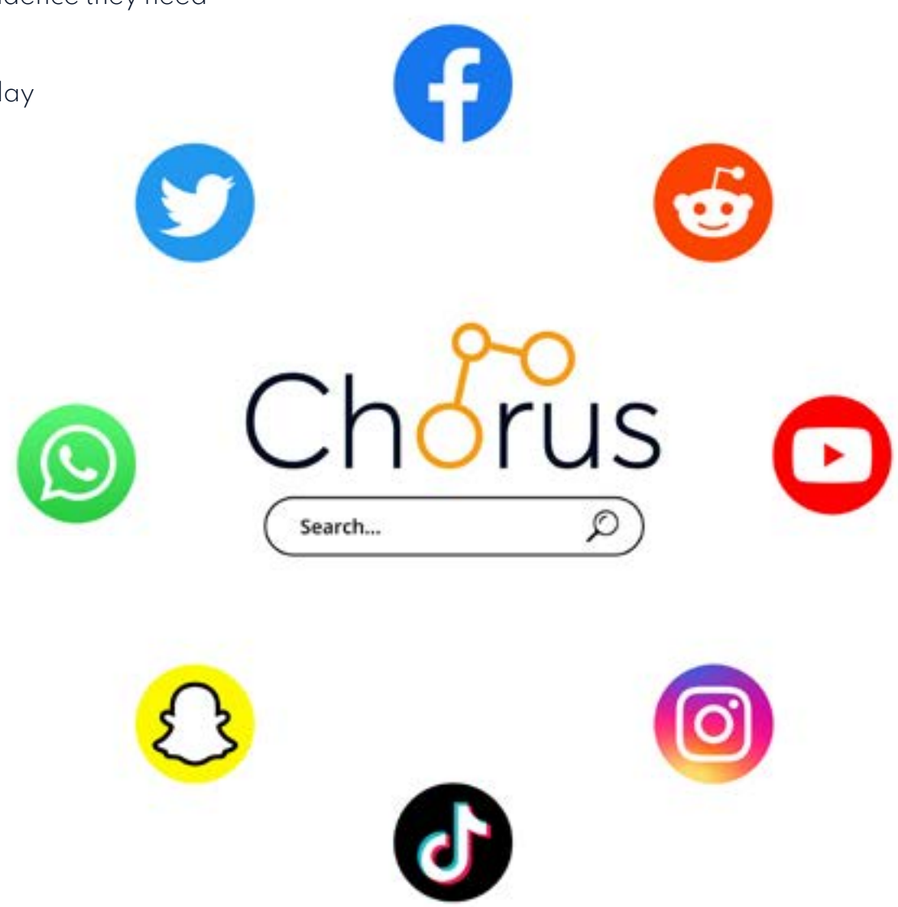
Federated Search & Enrichment

Bulk search across internal files, consented data and 200+ social media networks

The CIS features a leading entity enrichment tool. Query any entity, such as a name, phone number, email address and/or alias and search across all of your data sources to fast track the attribution process.

Federated and bulk searches can be performed across a number of data connectors, providing analysts, investigators and front line officers with the evidence they need to progress lines of inquiry.

Expand upon open-source intelligence in multiple ways and overlay with other forms of digital data in one interactive dashboard, to spot immediate connections.



"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 by

SHADOWDRAGON

Key features include:

- **Bulk search across internal files, consented data and 200+ 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, etc. to monitor emerging threats, optimize public safety and manage resourcing.
- **Go anonymous –** Leverage your covert social media accounts in an anonymous and secure environment.
- **Auto-matching –** Identify data in one case that has been previously captured in another.

Key benefits include:

- **Never miss a connection -** Customize your connectors relevant to your search query to perform bulk searches and reveal instant unknown intelligence.
- **Enrich your investigations -** Expand on data sets of relevance and perform advanced searches to interrogate further.
- **Get the full picture -** Overlay and visualize all of your digital data in multiple ways and in one dashboard, to spot connections.
- **Stay ahead of the game –** Ensure that key new information is captured immediately via watchlist alerts.

Entity enrichment and attribution tool

Secure Open-Source Capture

Capture internet intelligence instantly

The CIS features an advanced browser extension capable of capturing web pages, social media accounts, images and videos, in just one click.

Key evidence can then be stored as searchable files within your case in the CIS. Key capabilities include:

- **Go anonymous -** Log in to your covert accounts within the CIS and ensure your online footprint is hidden via a fully IP-obfuscated environment.
- **One-click capture -** Capture any digital intelligence, such as a webpage, social media account, image or video, in just one click. Choose to capture the whole page or just what is visible on the screen.
- **Redact, store and report -** Captures are stored as a searchable PDF or file within your case. Automatically redact names, numbers or any keyword from your captured evidence and add to a report.

One-click Capture





Internal Data Integration

Uncover hidden intelligence across your internal data

Securely upload any internal or unstructured, disparate legacy files into the CIS to centralize your investigative data.

Internal data integration will always ensure that your historic intelligence is always utilized. Key capabilities include:

- **Make your legacy data searchable** - Upload disparate data files via a secure upload portal. The CIS supports a range of file types including image-based PDFs that are fully searchable via OCR. All uploaded data will be indexed and made searchable.
- **Discover unknown connections** - Perform a cross-case analysis to determine if an entity, such as a name, phone number and/or address appears in any of your operational or closed cases.
- **Custom integrations supported** - Chorus can tailor specific integrations where the requirement exists. For example, a Record Management System (RMS) or any other line of business systems can be integrated and made searchable in the CIS.

Centralize internal and unstructured data





2409

Data Cleansing & Analysis

The most advanced data cleansing & analysis engine in the world

The CIS features an intuitive, self-serve, analytical dashboard to empower multiple roles, such as analysts, investigators and front-line officers, to get answers from their data, instantly.

Drag and drop any digital data files to be automatically cleansed and formatted.

Visualize, enrich and report on your data in multiple ways to spot connections and follow lines of inquiry.

Visualize, enrich and expand

Bring the data of your investigation to life through advanced visualization.

Overlay all relevant data for your case in one interactive dashboard to easily identify patterns around the time of an offense (e.g., plot phone and vehicle activity) on a map and overla with RF surveys and CCTV footage to understand the bigger picture.

Ingest and cleanse

Drag and drop any digital data into the CIS, to be automatically cleansed and formatted, saving 97% of your time.

Data types include: CDR's, ALPR, Handset Downloads, RF Surveys, Chat, Instant Messaging and more.



97%
time saved



Intelligent reporting

Choose from over 45 reports to query the most frequently asked investigative questions.

Produce maps, timelines, event schedules and charts to visualize the results in multiple ways (e.g., report on a suspects top 10 interactions or identify potential meetings between entities).

Evidential reporting

Overlay internal, external and consented data to interrogate and report in multiple ways



Generate courtroom ready reports

Present your digital evidence in a plethora of different formats and generate pre-populated or custom reports to courtroom ready standards.

- **Visualize, enrich and expand** - Generate interactive timelines, maps, pivot tables, heat charts and matrices to interpret your data in a multitude of ways to spot connections.

- **Intelligent Interrogation** - Choose from over 45 pre-populated reports to query the most frequently asked investigative questions, or set parameters and filters to answer your own custom query (e.g., Report on an individual's top 10 interactions or identify potential meetings between entities).

- **Customized reporting** - Easily combine your evidential data in a pre-configured or customized report. All evidential reports can be consolidated with individual disclosure reports; detailing a full audit log of how you collected, stored and captured data.

> "Chorus proved to be a valuable tool during the investigation and preparation for court."
>
> - Major Crime Investigator

Demo and free trial

Help us, help you. Trial the Chorus Intelligence Suite

Our promise

To assess and realize the maximum benefits of the Chorus Intelligence Suite, we offer free trials for all our products, to be used on your own live cases. All we ask is that you provide feedback on your experiences, so we can inform our development roadmap.

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



A dedicated Customer Success Manager to support you every step of the way

Why Chorus?

About us

Chorus Intelligence is a trusted supplier of data cleansing, analysis, search and entity enrichment software for law enforcement, government agencies, financial and corporate institutions across the globe.

Made up of one platform and a single user interface, the Chorus Intelligence Suite (CIS) can be used by all, no matter your role, to get answers from your data.

Founded in 2011, Chorus is used by 80% of UK police forces, all counter-terrorism units and many government agencies.

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 intelligence analysts who are experts in the Chorus Intelligence Suite.

Our experts

We combine former law enforcement analysts, investigators and open source experts with software developers that specialize in police and financial data.

Easy deployment

Chorus offers simple and secure cloud deployment to meet your custom requirements.

We partner with Amazon Web Services (AWS) Gov to offer a web-based, public cloud. We recommend AWS for organizations looking for a quick and easy set up.

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."

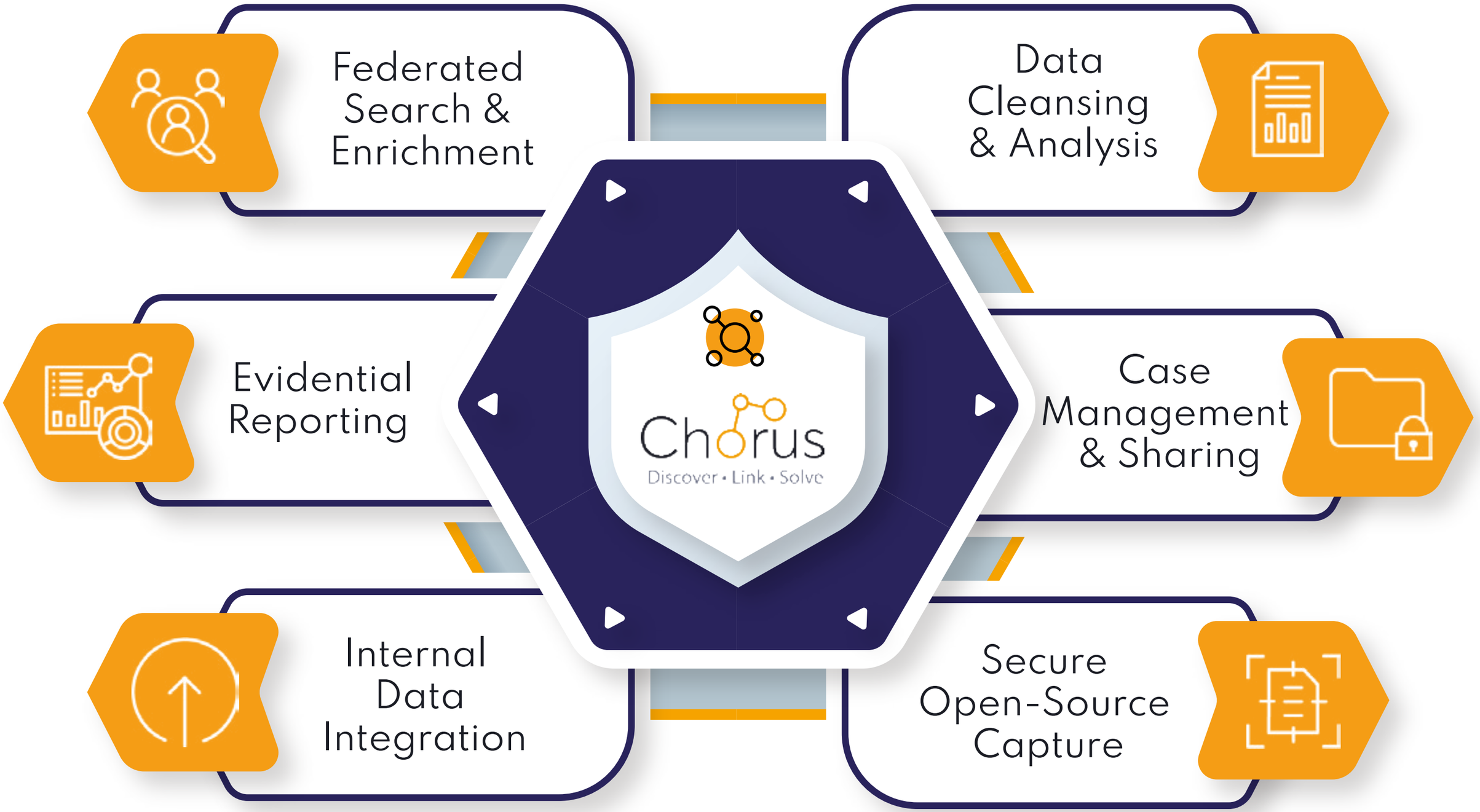
- Investigator

"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."

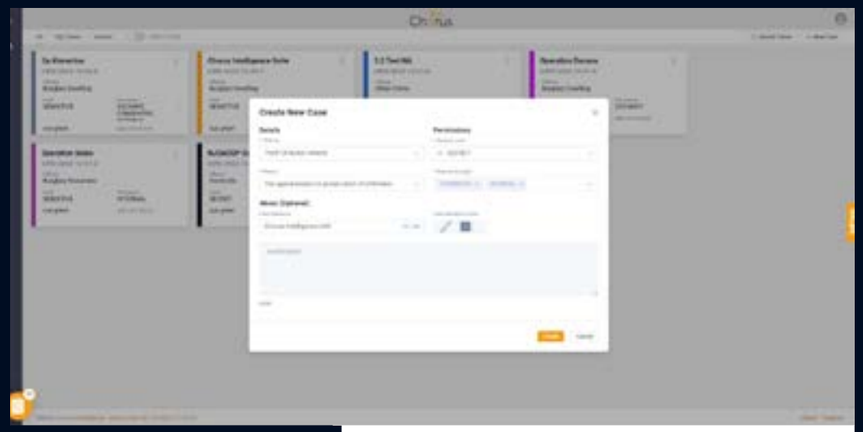
- Lead Analyst

"Chorus is by far the most significant aid to intelligence technology this century."

- Investigator

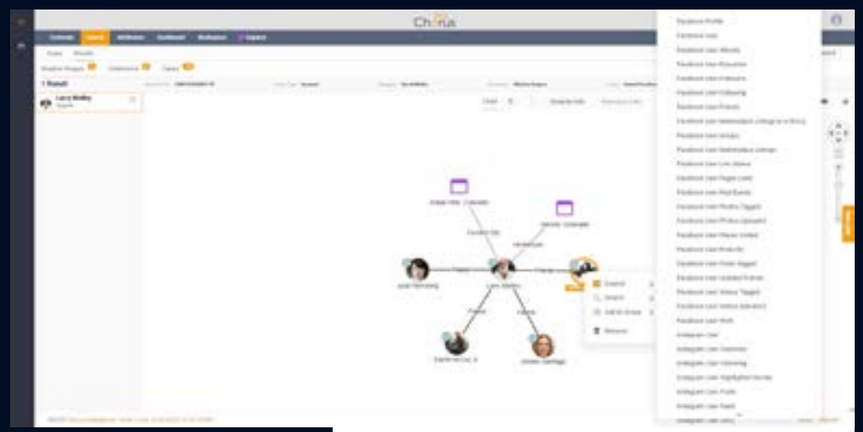

Federated Search & Enrichment
Data Cleansing & Analysis
Evidential Reporting
Case Management & Sharing
Chorus
Discover • Link • Solve
Internal Data Integration
Secure Open-Source Capture

The CIS at a glance



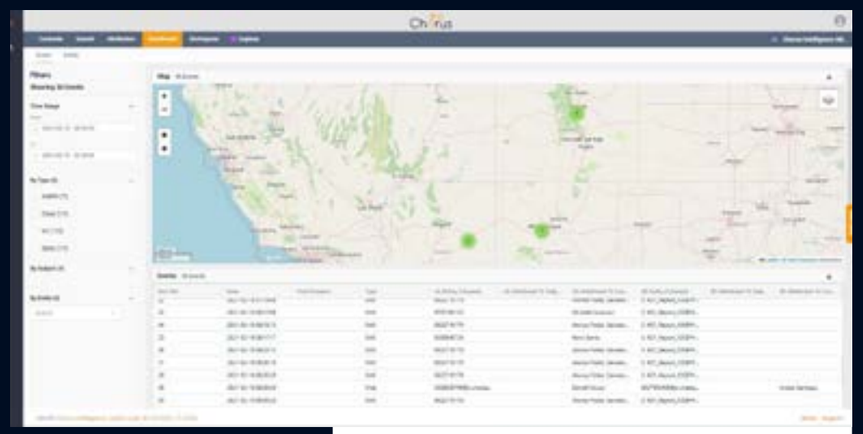
Case Management & Sharing

Create a case, store and share all investigative data in a central and secure digital hub.



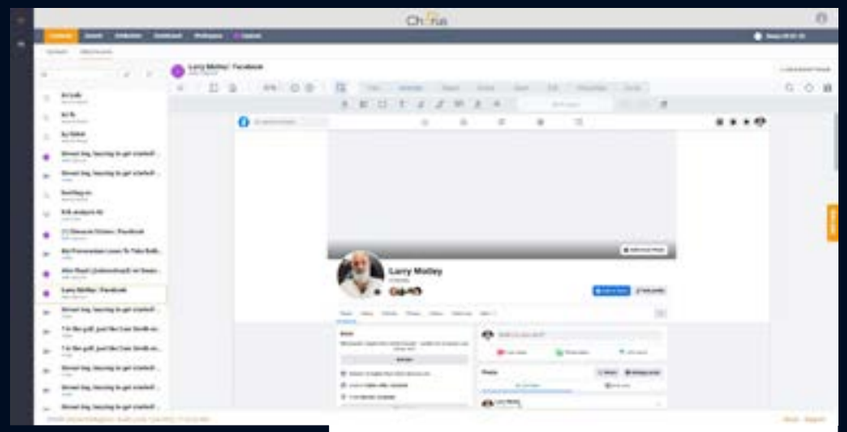
Federated Search & Enrichment

Query any entity and search across your internal files, consented data and over 200+ social media platforms.



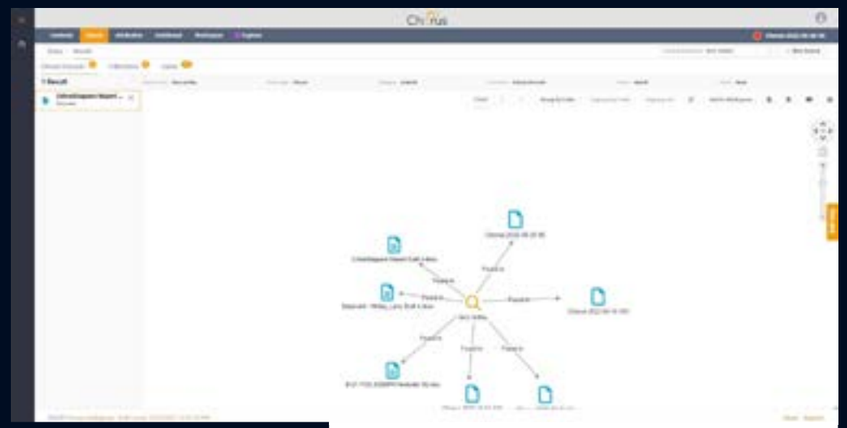
Data Cleansing & Analysis

Drag and drop any digital data to be automatically cleansed and formatted.



Secure open-source capture

Capture any webpage, image or video in a single click, from a secure and anonymous environment.



Internal Data Integration

Upload and index disparate data and make it searchable against your operational and closed cases.



Evidential Reporting

Overlay internal, external and consented data to interrogate and report in multiple ways.

Discover • Link • Solve

Contact

Chorus Intelligence Inc

4525 Main Street, Suite 710

Virginia Beach

VA 23462

Request a demo or free trial

NAsales@chorusintel.com

888 688 6842

chorusintel.com

Chorus

Discover • Link • Solve

Citigraf overview

Genetec Citigraf™

Citigraf Real-Time Crime Center provides situational intelligence to improve public safety. An effective public safety strategy involves proactively dealing with crime. Disorganized and siloed data inhibits collaboration across teams and slows down incident response times. Therefore organized, and consolidated data is crucial for a proactive approach to policing. Genetec Citigraf™ is a real-time situational awareness support system that unifies data streams and operations across city departments. Citigraf disseminates timely information and provides greater situational awareness to law enforcement agencies.

The open nature of our platform will enable the RTCC to consolidate policing data across department and regardless of the subsystems or sensors used. The end goal is for your staff to have access to the data they need, wherever they need, from one simple and intuitive platform. Additionally, our auditing and cybersecurity tools ensure the system is only used for its intended purpose and that all data collected and shared remains secure.

Our feature set, partnerships, and existing integrations give you a flexible toolbox that you can scale to your needs and a platform on which you can build future operational improvements.

Advanced GIS & ESRI mapping

Citigraf supports vector-based maps (ESRI/ArcGIS, Google, Bing, PDF), PTZ control and field of view, and customizable entity states.

Real-time situational awareness & investigations

Gather context for first responders by correlating data from sensors, cameras, and other systems in one simple map-driven user interface.

Post-incident investigations

Use video playback in correlation with ALPR, video analytics, and other sensor data to quickly gather insights about past incidents.

Video analytics

Ingest video analytics from cameras, including forensic search. Run server-based video analytics with direction control, object detection, stopped vehicle detection, camera integrity, people counting, and privacy protection. Integrate with third-party video analytics, such as Briefcam.

Video management

Supported by our globally top-ranked video management system. Benefit from possible integration to thousands of camera models for video streaming and control, edge video analytics, and varied functionalities for both streaming and playback.

License plate recognition

Leverage rich data from your Genetec Sharp and third-party ALPR cameras to provide additional situational awareness.

System federation

Connect multiple Genetec systems on a single front-end and federate other ALPR systems for greater investigation capabilities.

Interfaces for all user types

Unlimited users can access Citigraf on desktop, mobile, and/or web client.

Active directory (ADFS)

Allow single sign-on for user accounts across all Genetec platforms.

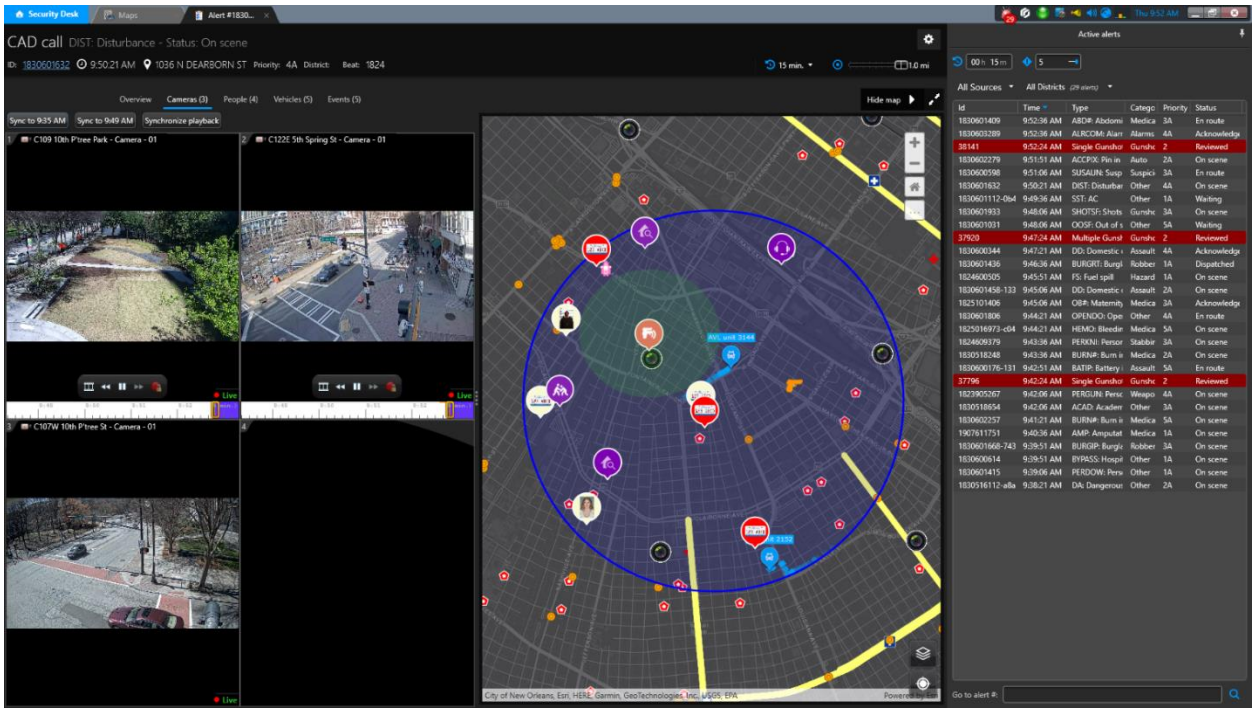
Community Connect integration

Integrate your Community Connect program by displaying the location of privately-owned cameras on your mapped interface, and the video streams of the cameras connected to your systems for both streaming and playback.



2417

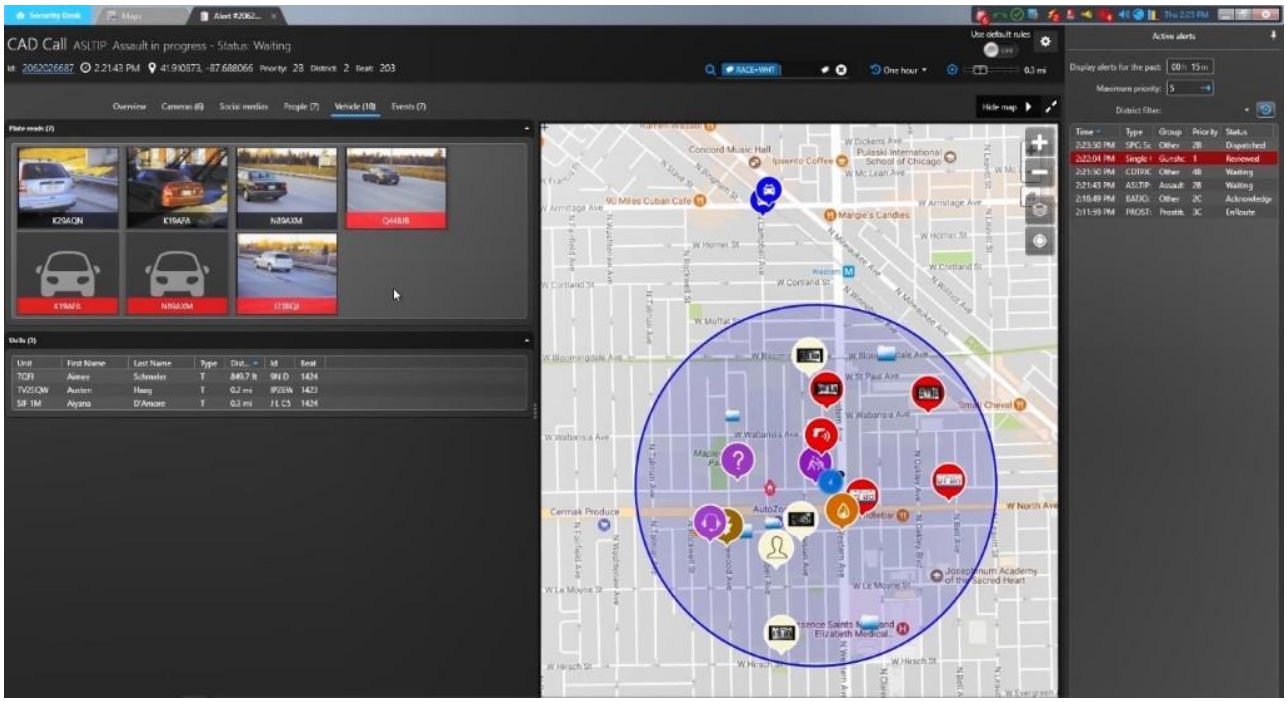
Citigraf™ Overview





2418

Citigraf™ Overview

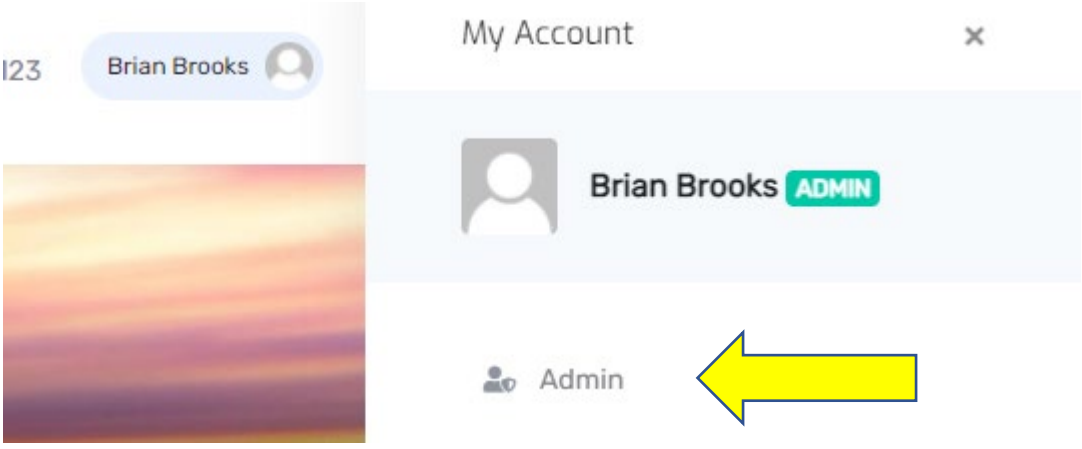


CNC LIVE How to Create an Event

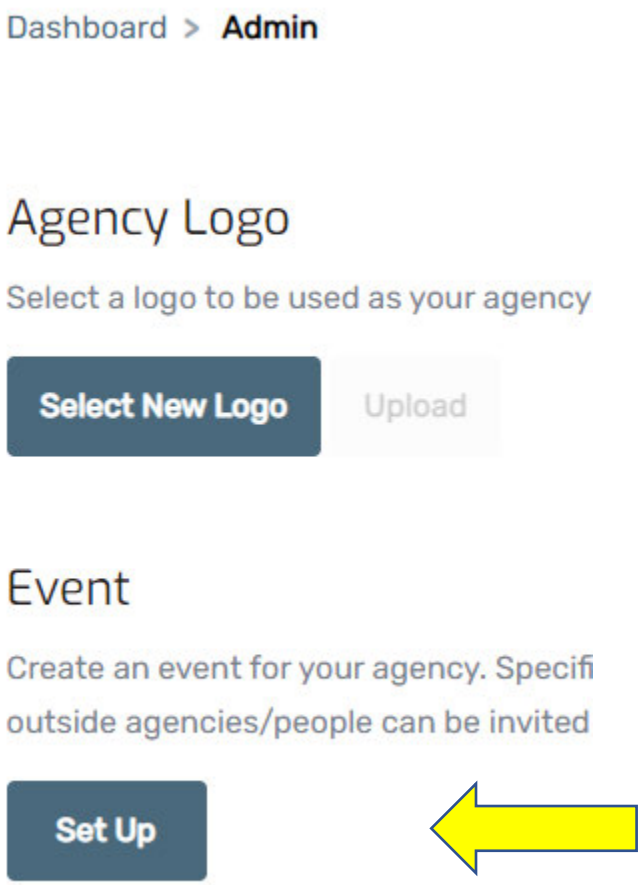
Through CNC Live MSP Air Wing personnel have the ability to grant temporary access to a user (Duty Officer, Patrol Supervisor or Local Officer) to view the Air Wing video feed. The Lieutenants in the Watch have the ability to serve as a backup in this function or primary if the Air Wing needs assistance.

Prior to "creating an event," Watch Lieutenants should check with the Air Wing and see if they have already created an event. Anytime the Air Wing is flying they will have someone on the ground monitoring, so that trooper is the primary for creating an event. The Air Wing feed is in real time. All Lieutenants in the Watch have Admin rights, so they have the ability to create temporary access to the video feed for a finite period.

First - Log into CNC live, once on the "Home Screen," **click on your name in the upper righthand corner of the screen**, that will open up a "sidebar." **Click on "Admin" <u>below your name in the sidebar</u>**, that will open up a new screen. (See below)



You are now on the Dashboard – Admin page. On the left-hand side of the screen you will see "Event" and under that is "Set up" in bold. **Click on the "Set Up" box**. (See below)



This will take you to a new page, Dashboard – Admin – Create Event, where you can "edit / update / or create a new event."

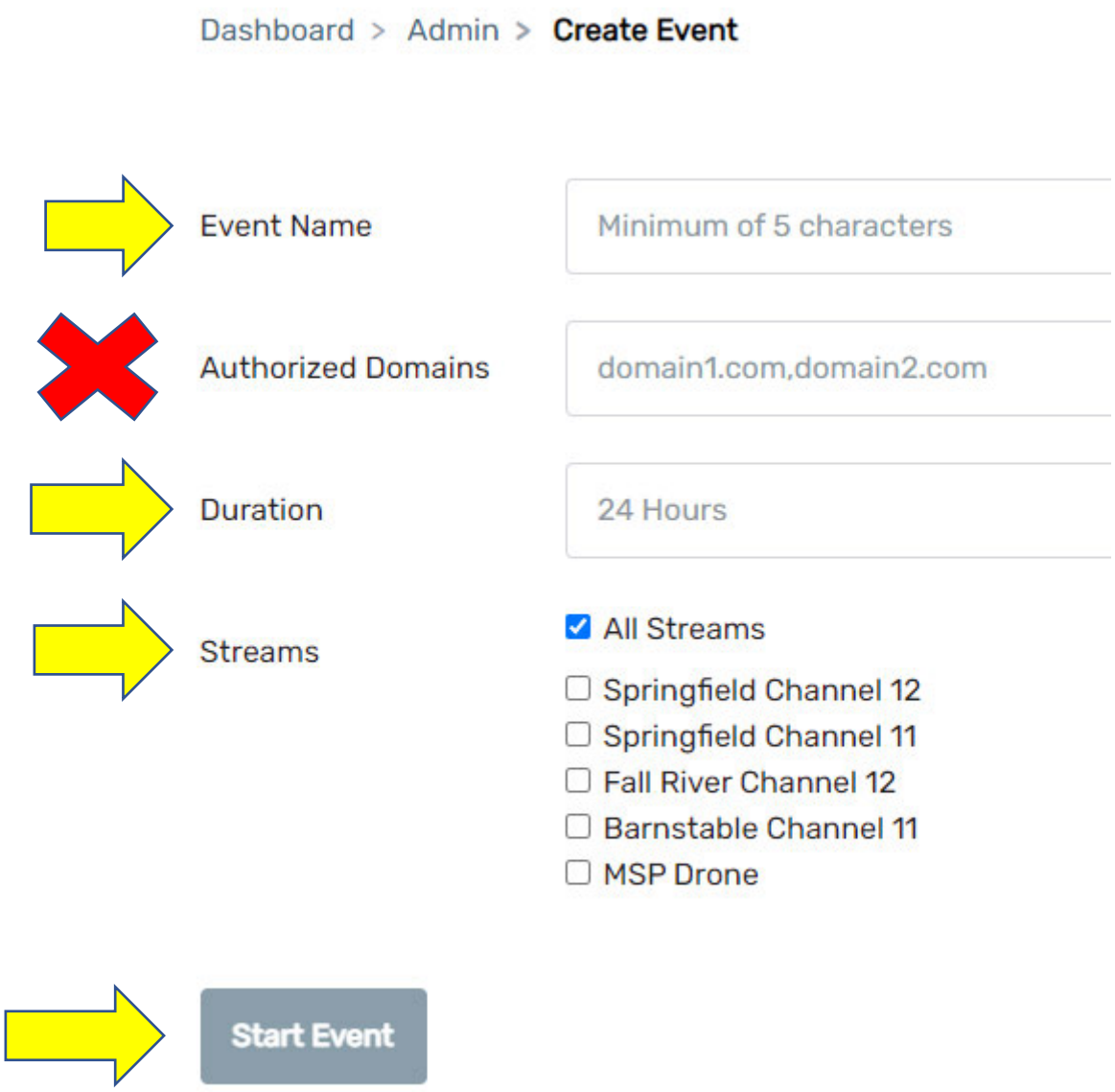
Next to "Event Name," **create an event name** (must be more than 5 characters)

Leave the "Authorized Domains" box alone. Don't enter anything here!

Next to "Duration," a dropdown will appear and **select the duration**

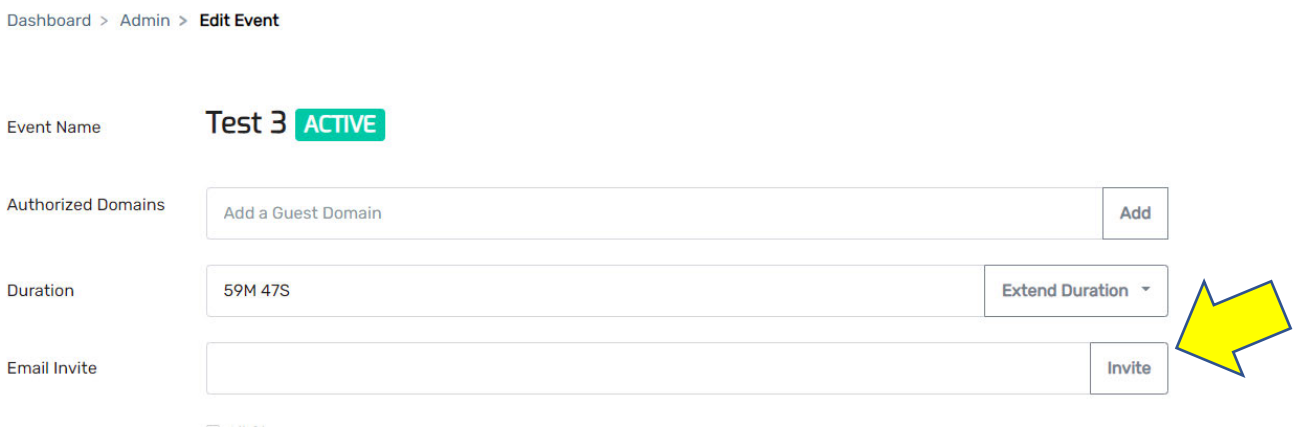
Next to "Stream," **check the Streams or channels you anticipate using**

Click the "Start Event" box at the bottom of the screen. (See below)



This will create a pop-up window asking if you want to start your event, **click the "Confirm" box**.

This will open a new page, Dashboard – Admin – Edit Event, the third box down says, "Email Invite." Next to the "Email Invite" box, **type in the user's email** and **click "Invite"** at the end of the box.



The user will then get an email and all they need to do is click the box that says, "View Event." Once they click the view event button, a CNC Live webpage will open containing the user's email in the "Email box" and a code in the "Key" box.

The user will **click the "Log In" box**. The user will then see the Streams or Receivers you previously selected.

You can send additional invitations by adding emails to the "Email Invite" box on the Dashboard – Admin – Edit Event page and clicking "Invite."

VIGILANT VEHICLEMANAGER QUICK GUIDES

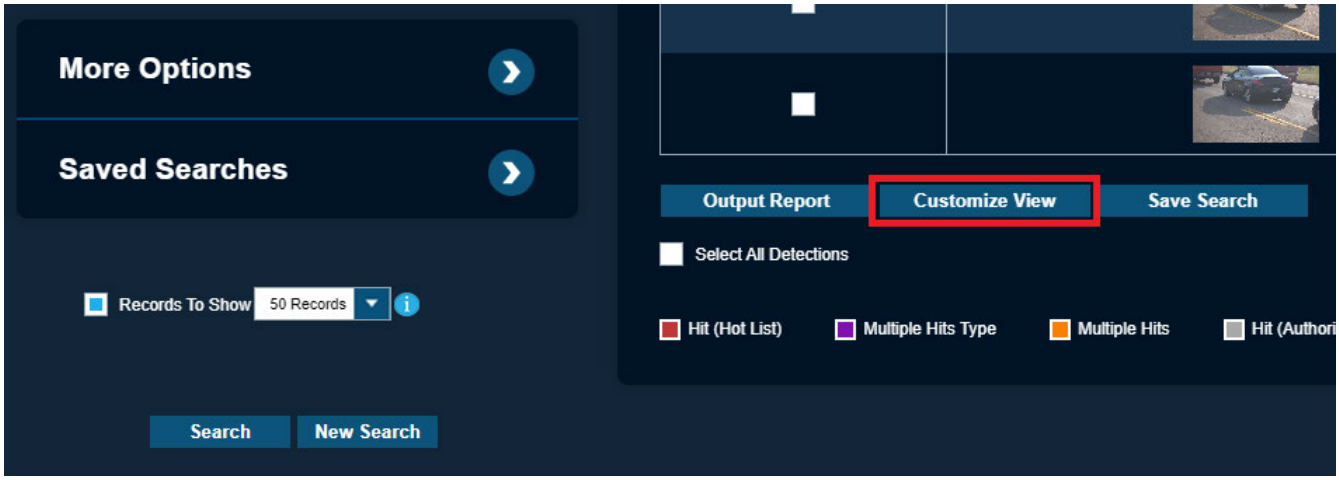
CUSTOMIZING QUICKSEARCH VIEW

This guide describes how Users can use the **Customize View** feature of QuickSearch to add or remove types of information from the QuickSearch results to make the presented information more useful at a glance.

- **Customize View** is a feature of VehicleManager that can be used to change the types of information presented on most pages that have search results.
- **QuickSearch** is the main search utility for LPR records in VehicleManager.

Custom views can be saved and selected later to create presets for different purposes.

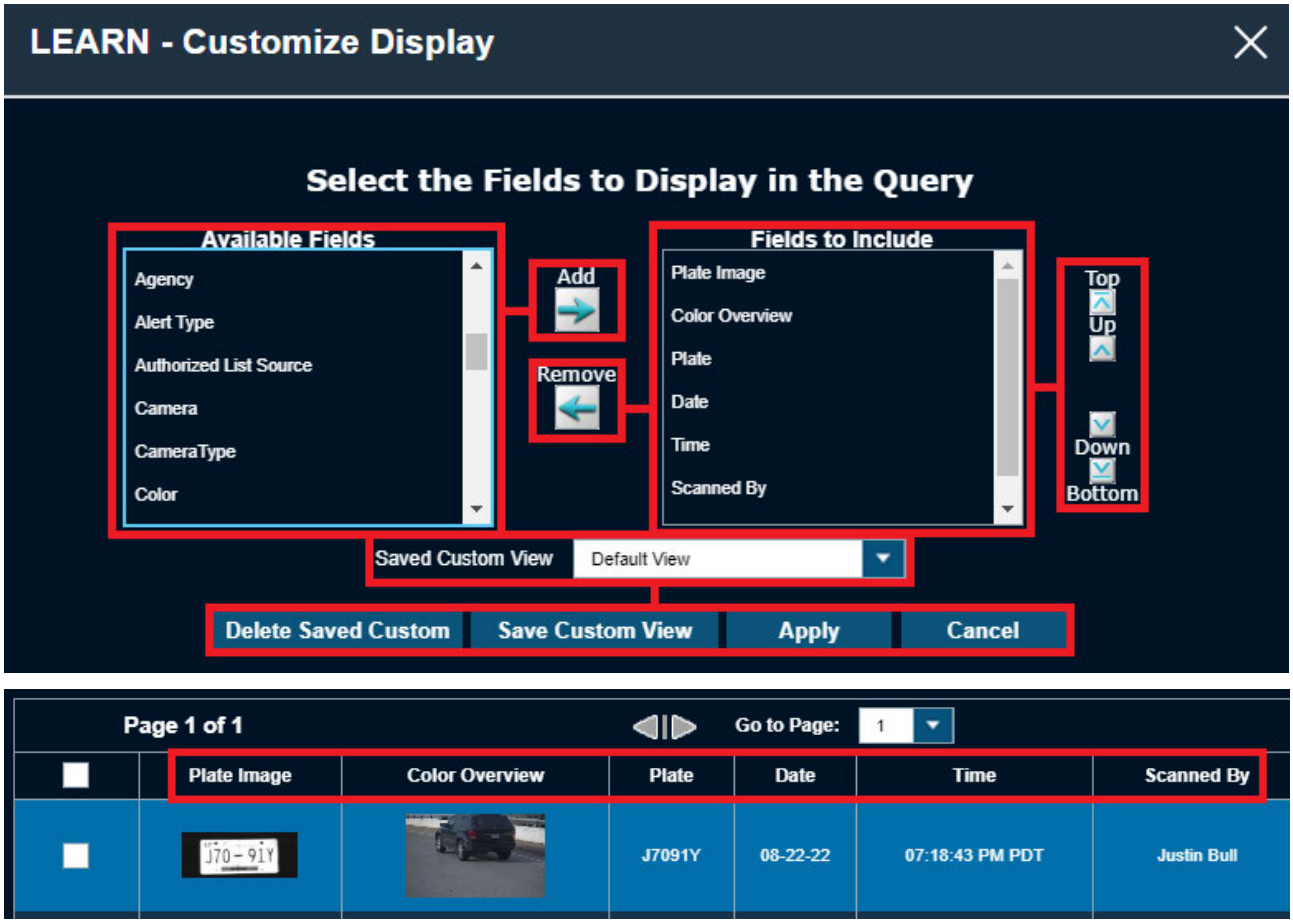
LOCATING CUSTOMIZE VIEW IN QUICKSEARCH



1. Login to Vigilant VehicleManager and navigate to **License plate query** → **Quick search**.
2. Click **Search**. Click on **Customize View**.

© 2023, Motorola Solutions. All rights reserved. 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.

USING CUSTOMIZE VIEW WITH QUICKSEARCH

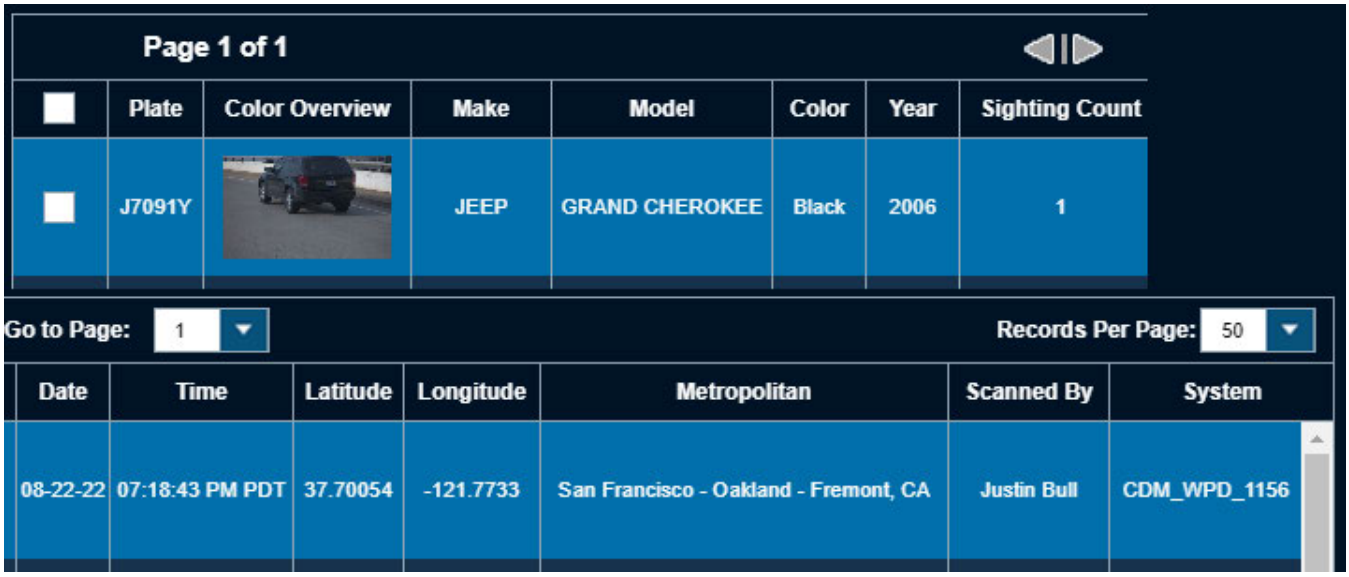


1. Under **Available Fields**, click on the information type to add to the QuickSearch results. Click **Add** to move it to the **Fields to Include** list.
2. Under **Fields to Include**, click on the information type to remove from the QuickSearch results. Click **Remove** to move it to the **Available Fields** list.
3. Use the **Up** and **Down** arrows to change the order of the selected information type in the **Fields to Include** list. Use the **Top** and **Bottom** arrows to move it to the top or the bottom of the list.

   NOTE: The information types displayed in the QuickSearch results will follow the order of the list, arranged from left to right.
4. Click **Save Custom View** to save the current configuration to the **Saved Custom View** drop down list.
5. If desired, select a Custom View from the **Saved Custom View** drop down list and click on **Delete Saved Custom** to remove it.
6. Click **Apply** to display the selected information types from the **Fields to Include** list in the QuickSearch results.

© 2023, Motorola Solutions. All rights reserved. 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.

USEFUL INFORMATION TYPES



Some useful Custom View information types to use in QuickSearch results are:

DEFAULT:

- **Color Overview**: A wide view image of the entire vehicle.
- **Plate Image**: A tight image of just the vehicle's license plate.
- **Plate**: The plate number as read by the camera.
- **Date**: The date the detection was made.
- **Time**: The time of day that the detection was made.
- **Scanned By**: The user logged in to the system that made the detection.
- **System**: The name of the system that made the detection.

LAW ENFORCEMENT (ADDITIONS):

- **Make**, **Model**, **Color**, **Year, Reg. State**: Vehicle type information.
- **Latitude**, **Longitude**, **Metropolitan Area**, **Detection State**: Location of the detection.
- **Sighting Count**: The number of times the vehicle has been detected.

PARKING (ADDITIONS):

- **Sighting Count**: The number of times the vehicle has been detected.
- **Agency**: The agency that owns the systems that made the detections.
- **Alert Type**: The alert type assigned to the vehicle if it is on a Hot List.
- **Authorized List Source**: The name of the Authorized List source that this vehicle is on.
- **Time Exceeded**: This vehicle has an expired permit.
- **Validated**: This vehicle's permit has been marked as valid.

© 2023, Motorola Solutions. All rights reserved. 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.

Department of State Police
DIVISION COMMANDER'S ORDER

Issue Date	**Number**
September 13, 2023	**2023-DHS-013**
Subject: **ALPR Data Retention & Access**	

The Division of Homeland Security and Preparedness is responsible for the administration of the Department's Automatic License Plate Recognition (ALPR) system. The availability and use of ALPR technology significantly enhances public safety by augmenting the operational and investigative effectiveness of law enforcement agencies.

The use of ALPR technology is governed by General Order TRF-11 "Automatic License Plate Recognition". In addition, the use of ALPR systems shall be subject to the guidelines set forth in this Order unless superseded by General Order TRF-11.

Pursuant to General Order TRF-11, the retention of ALPR data collected by the Department shall be determined by the Department of Criminal Justice Information Services (DCJIS) policy. Furthermore, ALPR systems operated by the Department shall be configured to restrict data visibility for a maximum duration of sixty (60) days from the date of the initial request.

Users requesting to access records beyond sixty (60) days, shall contact the Commonwealth Watch Center, the ALPR Administrator, or other administrator authorized by the Division Commander of Homeland Security and Preparedness. The request will be reviewed on a case-by-case basis. In the absence of exigent circumstances, the user may be required to revise their request, consult with a District Attorney's Office of jurisdiction, or to submit legal process to obtain the requested records.

_____

Mark D. Cyr
Lieutenant Colonel
Division of Homeland Security and Preparedness

Department of State Police
DIVISION COMMANDER'S ORDER

Issue Date	**Number**
September 13, 2023	**2023-DHS-013**
Subject: **ALPR Data Retention & Access**	

The Division of Homeland Security and Preparedness is responsible for the administration of the Department's Automatic License Plate Recognition (ALPR) system. The availability and use of ALPR technology significantly enhances public safety by augmenting the operational and investigative effectiveness of law enforcement agencies.

The use of ALPR technology is governed by General Order TRF-11 "Automatic License Plate Recognition". In addition, the use of ALPR systems shall be subject to the guidelines set forth in this Order unless superseded by General Order TRF-11.

Pursuant to General Order TRF-11, the retention of ALPR data collected by the Department shall be determined by the Department of Criminal Justice Information Services (DCJIS) policy. Furthermore, ALPR systems operated by the Department shall be configured to restrict data visibility for a maximum duration of sixty (60) days from the date of the initial request.

Users requesting to access records beyond sixty (60) days, shall contact the Commonwealth Watch Center, the ALPR Administrator, or other administrator authorized by the Division Commander of Homeland Security and Preparedness. The request will be reviewed on a case-by-case basis. In the absence of exigent circumstances, the user may be required to revise their request, consult with a District Attorney's Office of jurisdiction, or to submit legal process to obtain the requested records.

_____

Mark D. Cyr
Lieutenant Colonel
Division of Homeland Security and Preparedness

Streamvault SV-300E

All-in-one security appliance

The Streamvault™ SV-300E all-in-one security appliance helps you move to a unified system combining video surveillance, access control, intrusion, and communications more efficiently. It combines all the capabilities you need to secure a small site in a single device, simplifying both installation and maintenance.

Guaranteed performance

- up to **32** cameras
- up to **100** readers
- up to **32** ALPR cameras
- up to **60TB** storage



Key features

- Turnkey appliance with Genetec™ Security Center pre-installed
- Local recording and monitoring of video, access control, and other security events
- Machine learning endpoint protection
- 3-year hardware warranty with 1-year advance replacement

Benefits



Speed up your deployment – Get your security system up and running quickly and efficiently with Security Center pre-installed and built-in wizard-based tools to configure your system.



Protect your security system – Streamvault appliances help you build a resilient security system that protects your data and operations. Our cyber security experts stay vigilant on evolving threats and help identify and address new vulnerabilities promptly.



Reduce your system's footprint – With Security Center and the SV-300E, you can consolidate video, access control, intrusion detection, and other security systems on a single device.

Applications

Retail

Standardize your processes across your entire chain. The Streamvault SV-300E appliance lets you record and monitor video locally, and makes it easy to connect remote sites with a centralized location.

Education

The Streamvault SV-300E series lets you monitor entries and exists with unified video and access control, so you can keep staff and students safe across your school.

Banking

Combine video, access control, and intrusion systems in a single platform and enhance security across your installations.

Technical specifications

OS
Windows 10 IoT Enterprise LTSC 2019

Processor
SV-300E : Intel® Core™ i5
Passmark: 13346

Memory
16 GB DDR4

Ethernet
SV-300E: Onboard 1 GbE RJ45

Peripherals
SV-300E : 4x USB 3.0 + 4x USB 2.0

Display
SV-300E: 1x HDMI + 1x DisplayPort

Mechanical and environmental

Operating temperature
50°F to 95°F (10°C to 35°C)

Operating humidity
5 - 90% (non-condensing)

Certifications
Regulatory IEC 60950-1, European Norm EN 60950-1, CISPR 22/CISPR 24, EN55022/55024

Storage

Drive type
3.5” Dell Enterprise SATA drives

OS drive
1x 256 GB 2.5” SSD

Maximum data storage
60 TB

Cybersecurity

Endpoint protection
BlackBerry Protect machine learning antivirus

Hardened image
200+ security settings changed by default

Maintenance
Verified Windows updates
Connected services for Genetec software and device firmware updates

Warranty and support

Hardware warranty
3-year warranty with 1-year advance replacement and next business day on-site service

Security Center support
Latest version

Models

Model	Form factor	Dimensions (W x D x H)	Weight	Power supply
SV-300E	Small form factor	3.7” x 11.5” x 11.4” (97 mm × 292 mm × 290 mm)	11.4 lbs (5.1 kg)	1x 200W
SV-300E-T4	Tower	6.95” x 13.58” x 13.19” (176.6mm x 345mm x 335mm)	25.7 lbs (11.7 kg)	1x 460W

*Hardware specifications are subject to change. Units provided will be equivalent or superior to what is shown in this document.

Genetec Inc.
genetec.com/locations
info@genetec.com
@genetec

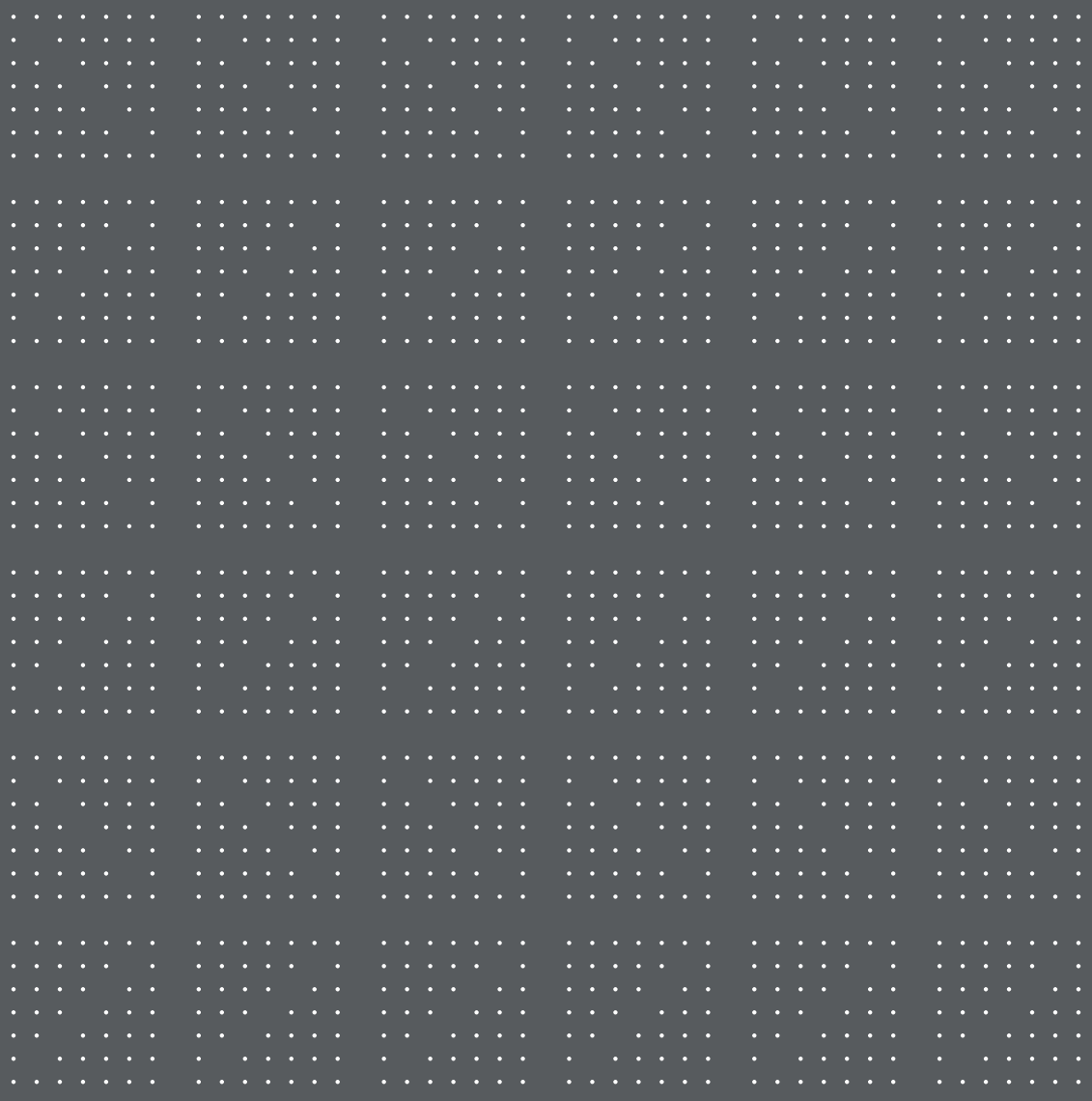
© Genetec Inc., 2023. Genetec, Streamvault and the Genetec Logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions. Other trademarks used in this document may be trademarks of the manufacturers or vendors of the respective products.

UPTD_MAY2019

2430

Genetec Citigraf™

Comprehensive response coordination



Genetec™

See your city through a shared lens

Every day, law enforcement officers and emergency responders are working together to keep our cities and communities safe. But the realities of public safety are rapidly evolving, and the risks to cities are multiplying.

The task is made increasingly difficult by a growing array of sensors and solutions capturing data that can't be meaningfully integrated into everyday city operations. Often, responders lack a clear perspective on incidents, making coordination and collaboration difficult when shared information could improve effectiveness.

Genetec Citigraf is a decision support system that empowers public safety departments to build a deeper, data-driven understanding of what's happening in their city. Whether it's receiving an emergency call, responding to incidents, or ensuring public safety at an event, Citigraf provides a common operating picture so your personnel can make better decisions based on timely information.

Citigraf correlates and displays incoming data through dynamic maps, supporting operation centers and frontline personnel with deeper situational awareness as events unfold. They can act based on insights, share relevant information, and coordinate efforts more easily.

Following an event, managers can review responses, train staff, and improve planning and resource management. With Citigraf, they can manage every type of situation – from the unexpected to the everyday.

2433

Gather data from different sources

To this day, operators struggle to make sense of an array of incoming data. Coordinating a response is often a disjointed and time-consuming process that makes it difficult to provide valuable situational awareness to other agencies and first responders.

Citigraf changes all that. It allows you to collect and quickly analyze data from multiple sensors and systems, and use it to build a better understanding and coordinate operations.

Rely on a shared view of the city

Citigraf gives multiple agencies the ability to access, visualize, and direct assets and resources using a common operating picture. They tap into the same, relevant data sources, which allows them to gain a better view of events so they quickly respond to – and gain control of – situations.

Citigraf breaks down silos by displaying relevant and useful information to help multiple agencies act together rather than as individual entities. Through its intuitive interface based on dynamic city maps, command center staff get a complete overview of real-time and historical data. It provides better situational awareness, and empowers operators to make better, faster, more informed decisions.

Derive data-driven intelligence

Once data has been gathered, knowing how to make sense of it is essential. Citigraf continually analyzes information from thousands of sensors and data points, assisting frontline public safety teams by bringing to light relevant events and information.

The Citigraf correlation engine assesses both temporal and geospatial data to prepare responders for what they can expect before arriving onsite. It allows individuals and agencies to see the full landscape of what's happening across the city.

Learn through deeper understanding

After an event, use the knowledge acquired to refine prevention plans, response strategies, and resource management. Gauge the effectiveness of initiatives, and better train and teach your team to prepare for future situations.

For instance, based on historical data, you might recognize that car theft increases in the area where city visitors are staying in the days leading up to an annual public event. Equipped with that insight, police officers can be dispatched in that area to decrease that threat at future events.



An investment in public safety

Those in charge of protecting the public must deal with the dual challenge of managing both large-scale public events and unexpected situations. Let's look at two examples of how Citigraf can help decision makers safely manage and coordinate events – an annual parade, and a city flood.

The city's annual parade

Summer is a busy time for the city. The parade is one of the biggest events in the calendar, as the police, fire, and emergency operations prepare for an influx of visitors to add to the many thousands who already call the city home.

The heart of operations is the command center. The Citigraf application is used to manage the event and coordinate on-site personnel such as public workers, emergency operations staff, police officers and firefighters.

During the event planning phase, data relevant to the event is used to identify trends, and it is subsequently used to identify opportunities for future improvement.

As the event begins, all agencies coordinate with the command center for live operations. Information comes into Citigraf from event staff, patrol cars, officers on the street, automatic license plate

recognition (ALPR) systems, and cameras around the parade route. Video, event data, CAD, and emergency calls are all instantly available, analyzed, and correlated by Citigraf to optimize operations, response times, and mitigation of incidents. Critical situations around the event – from crimes to medical emergencies – are managed more efficiently.

22%

The decrease in shootings seen in one year in Chicago districts that have deployed Citigraf in their decision support centers.

The cross-departmental team can see a comprehensive map of the city delivered by Citigraf. They share the same view with the Chief of Police and the different agencies, and they have access to all cameras around the parade route, so they know exactly what's going on. Every point of data is geo-localized, so they know where everything is happening. They can see real-time information that previously wouldn't have made it into the command center until after the event. So, when an incident happens, they can quickly coordinate resources before, during, and after – and effectively respond.

After the event, decision makers can see what has transpired to help them plan for a safer, smoother event next year.

The threat of flooding

Floods can happen fast and they can be devastating. It's essential to be prepared for every eventuality and to have the capacity to act quickly.

A flood alert has been released by the weather service. The Chief of Police remembers the last time there was a flood in the city. A tropical storm had swept through and flooded the northern suburbs of the town. Back then, they recorded everything by writing things down. They didn't have the necessary data to analyze their response so they could improve operations in the future. This time, they are better prepared.





2440

39%

The reduction of on-scene arrival times in one of the most at-risk Chicago districts since Citigraf has been rolled out.

Using Citigraf, operators are notified about the developing situation, while the command center can view weather data on the map of the city, helping them easily identify the areas most at risk.

As the flood approaches, a clear picture of the situation begins to emerge in Citigraf. The team keeps a close eye on the weather and hydrology forecasts while monitoring the water level of every connected river, stream, and tributary. They can see how the tracks are forming, and which roads might need to be closed.

> ‘Through Citigraf, information can be dispatched quickly and efficiently to first responders attending to the people and areas in need.’

Through unified access to surveillance cameras and social media, the level of risk can be confirmed. Rich, visual layers of data on the map show major buildings or public areas that are without power or in need of evacuation. This essential information provides emergency responders with insights about the citizens who are most at risk. Through Citigraf, information can be dispatched quickly and efficiently to first responders attending to the people and areas in need. Emergency vehicles can see which roads to take, and which roads have been closed.

Once the water has subsided and the clean-up operation is underway, the incident managers can begin looking at how things unfolded to learn from the experience. They can train their teams, and share invaluable information that will help save lives.

Who's using Citigraf?



Law enforcement agencies
Chiefs of police, county sheriffs, fusion center directors, and state police commanders are equipped with the right tools to analyze and correlate data on a temporal and geospatial basis. It allows them to identify potential links and trends that affect crime levels and the safety of their communities.



Emergency management
The system can automatically prioritize relevant data as it is displayed in a simple way to enable a coordinated response. This gives emergency management the ability to effectively and quickly identify, respond to, and gain control of situations.



City officials
Mayors, governors, city councilors, and executives can reduce the cost of delayed responses. And, through better documentation of events, they can better communicate the effectiveness of first responders and their departmental budgets.

The benefits of Citigraf

A common operating picture
Tap into data from disparate systems and get access to data from video and ALPR cameras, CAD calls, digital maps, record management systems, weather reports, and a variety of sensors deployed throughout the city. Facilitate cross-agency communication based on a common operating picture.

Quicker access to relevant, correlated information
Get relevant information at the right time. Based on geospatial and temporal criteria, your system instantly detects and displays all relevant information from cameras, people, vehicles, and events that require immediate attention.

Use existing data to derive insights and help decision making
See incident trends emerge through an advanced operational analytics platform, with a correlation engine that connects searches across global databases. It will help you measure the effectiveness of initiatives, understand the evolution of incidents across the city, and be better prepared for major events.

A unified system, a coordinated response

Citigraf is a decision support system that allows cities, law enforcement, and emergency responders to work together to plan for, identify, and respond to events and incidents. It unifies public safety operations through situational awareness and the proper dissemination of information. A reduction in threats and better preparedness for what might happen lead to strengthened public safety, and an increase in the quality of life in local communities.

Corporate Headquarters
Genetec Inc.
2280 Alfred-Nobel Blvd.,
Montréal QC H4S 2A4
Canada
Toll Free: +1 866 684 8006
Canada & USA:
Tel: +1 514 332 4000
genetec.com

© Genetec Inc., 2017
Genetec and the Genetec logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions.

All images are used for illustrative purposes only

Genetec Citigraf empowers public safety agencies to share a common operating picture to help them prepare for, manage, and respond to situations – from the unexpected to the everyday.

STATE OF CONNECTICUT

DEPARTMENT OF EMERGENCY SERVICES AND PUBLIC PROTECTION

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE CONNECTICUT DEPARTMENT OF EMERGENCY SERVICES AND PUBLIC PROTECTION
AND THE
TOWN OF MARLBOROUGH, POLICE DEPARTMENT
CONCERNING ACCESS TO VEHICLE RELATED INFORMATION IN THE NCIC SYSTEM FOR THE LICENSE PLATE READER PROJECT

I. PURPOSE

The purpose of this Memorandum of Understanding (MOU) is to document agreed responsibilities and functions of the Connecticut Department of Emergency Services and Public Protection ("DESPP") and the Town of Marlborough Police Department ("Town"), hereinafter, "the parties," with respect to the access, transmission, use, and storage of information from the License Plate Reader (LPR) hotlist and the National Crime Information Center (NCIC) System as retrieved through the LPR system.

II. AUTHORITIES

The DESPP enters into this MOU under the authority of Connecticut General Statutes (C.G.S.) § 4-8 and Chapters 528 and 529, *et seq*. The Town enters into this MOU under the authority of C.G.S. § 7-130d.

III. BACKGROUND INFORMATION

LPR systems utilize specialized cameras to capture license plate images and use computers to perform Optical Character Recognition (OCR) on those images such that the OCR values can be compared to a stored list of license plates values. The stored license plate value list is referred to as a hot list. The hot list contains license plate values associated with vehicles having significance to law enforcement, such as license plates associated with stolen vehicles, vehicles associated with wanted or missing persons, vehicles associated with AMBER/SILVER Alerts, as well as those reasonably believed to be involved with criminal activity. LPR systems include mobile LPR systems, mounted on police vehicles, and portable LPR systems that can be deployed in temporary stationary locations.

1111 Country Club Road
Middletown, CT 06457
Phone: (860) 685-8150/Fax: (860) 685-8354
An Affirmative Action/Equal Opportunity Employer

Town wishes to institute LPR technology from mobile and fixed sites that will allow DESPP to upload current information from NCIC and motor vehicle files. Vendors provide software and screening devices which have the capability to scan license plates and search local databases loaded into a patrol vehicle computer or other location controlled by the Town law enforcement agency.

IV. SPECIFIC RESPONSIBILITIES

1. DESPP will:

   a. Provide the Town LPR units with updated information from the LPR system database via the designated DESPP server.
   b. Provide the Town with the name and telephone number of a technical and an administrative point of contact (POC) for the LPR system;
   c. Designate a LPR System Administrator responsible for updating all LPR hotlists in a timely manner; and
   d. Ensure stored data is purged from the LPR system operations software ninety (90) days after it has initially been stored, subject to changing DESPP policies.

2. The Town law enforcement organization will:

   a. Use the LPR system information for law enforcement purposes only;
   b. Be responsible for the installation and maintenance of the LPR system equipment in vehicles, fixed, or temporary locations;
   c. Be responsible for any licensing costs, data usage and storage with vendors;
   d. Be responsible for any systems software purchase, installation, and maintenance costs;
   e. Ensure that software licenses are exactly synchronized with set DESPP expiration dates;
   f. Be responsible for officer training regarding use of the LPR system;
   g. Develop a LPR system policy for Town use;
   h. Create defined user roles and designate local and patrol-level system administrators, while ensuring that such users are maintained;
   i. Be responsible for the connection to the DESPP server through the Department of Administrative Services.
   j. In accordance with current NCIC "hit" confirmation procedures, confirm that extract matches against LPR scans are still active records in the NCIC System at the earliest reasonable opportunity.

k. Register all LPR devices with DESPP.
l. Not release NCIC data to any Vendors.
m. Report any data inaccuracies promptly to the LPR System Administrator.
n. Not release hotlists to any other municipal law enforcement agencies without written permission from DESPP.
o. Respond promptly to Freedom of Information Act requests if responsive material is available.

3. Both Parties agree:

a. Before using Personally Identifiable Information shared pursuant to this MOU, the recipient agency will make reasonable efforts to ensure the information is accurate, timely, relevant, and complete.

b. Each Party will immediately report to the other Party each instance in which data received from the other Party is used, disclosed, accessed in an unauthorized manner (including any data losses or breaches), or otherwise misused.

c. The FBI and/or DESPP may audit the handling and maintenance of data in electronic and paper recordkeeping systems to ensure appropriate security and privacy protections are in place.

d. The transfer of information described under this MOU will be conducted at the unclassified level and the transmission and storage of NCIC information will comply with the *CJIS Security Policy* and all relevant policy and regulations.

e. The Town shall indemnify, defend and hold harmless the State and its officers, representatives, agents, servants, employees, successors and assigns from and against any and all (1) Claims arising, directly or indirectly, in connection with the MOU, including the acts of commission or omission (collectively, the "Acts") of the Town; and (2) liabilities, damages, losses, costs and expenses, including but not limited to, attorneys' and other professionals' fees, arising, directly or indirectly, in connection with the MOU. The Town shall use counsel reasonably acceptable to the State in carrying out its obligations under this section. The Town's obligations under this section to indemnify, defend and hold harmless against Claims includes Claims concerning confidentiality of any part of or all of the Contractor's bid, proposal or any Records, any intellectual property rights, other proprietary rights of any person or entity, copyrighted or uncopyrighted compositions, secret processes, patented or unpatented inventions, articles or appliances furnished or used in the Performance. The Town shall not be

responsible for indemnifying or holding the State harmless from any liability arising due to the negligence of the State or any other person or entity acting under the direct control or supervision of the State.

f. The Parties acknowledge and agree that nothing in the MOU shall be construed as a modification, compromise or waiver by the State of any rights or defenses of any immunities provided by Federal law or the laws of the State of Connecticut to the State or any of its officers and employees, which they may have had, now have or will have with respect to all matters arising out of the MOU. To the extent that this section conflicts with any other section, this section shall govern.

g. This MOU is subject to the provisions of Executive Order No. Three of Governor Thomas J. Meskill, promulgated June 16, 1971, concerning labor employment practices, Executive Order No. Seventeen of Governor Thomas J. Meskill, promulgated February 15, 1973, concerning the listing of employment openings, Executive Order No. Sixteen of Governor John G. Rowland, promulgated August 4, 1999, concerning violence in the workplace, Executive Order No. 14 of Governor M. Jodi Rell, promulgated April 17, 2006, concerning procurement of cleaning products and services, in accordance with their respective terms and conditions; and Executive Order No.49 of Governor Dannel P. Malloy, promulgated May 22, 2015, which mandates disclosure of gifts to public employees and campaign contributions to candidates for statewide public office or the General Assembly for state contracts valued at more than $50,000, all of which are incorporated into and are made a part of the MOU as if they had been fully set forth in it.

h. The Town agrees and warrants that in the performance of the MOU such Town will not discriminate or permit discrimination against any person or group of persons on the grounds of race, color, religious creed, age, marital status, national origin, ancestry, sex, gender identity or expression, mental retardation, mental disability or physical disability, including, but not limited to, blindness, unless it is shown by such Town that such disability prevents performance of the work involved, in any manner prohibited by the laws of the United States or of the State of Connecticut; and the Contractor further agrees to take affirmative action to insure that applicants with job-related qualifications are employed and that employees are treated when employed without regard to their race, color, religious creed, age, marital status, national origin, ancestry, sex, gender identity or expression, mental retardation, mental disability or physical disability, including, but not limited to, blindness, unless it is shown by the Town that such disability prevents performance of the work involved; (2) the Town agrees, in all

solicitations or advertisements for employees placed by or on behalf of the Town, to state that it is an "affirmative action equal opportunity employer" in accordance with regulations adopted by the Commission; (3) the Town agrees to provide each labor union or representative of workers with which the Town has a collective bargaining Agreement or other contract or understanding and each vendor with which the Town has a contract or understanding, a notice to be provided by the Commission, advising the labor union or workers' representative of the Contractor's commitments under this section and to post copies of the notice in conspicuous places available to employees and applicants for employment; (4) the Town agrees to comply with each provision of this Section and Connecticut General Statutes §§ 46a-68e and 46a-68f and with each regulation or relevant order issued by said Commission pursuant to Connecticut General Statutes §§ 46a-56, 46a-68e and 46a-68f; and (5) the Town agrees to provide the Commission on Human Rights and Opportunities with such information requested by the Commission, and permit access to pertinent books, records and accounts, concerning the employment practices and procedures of the Contractor as relate to the provisions of this Section and Connecticut General Statutes § 46a-56.

V. EFFECT OF THIS MOU

This MOU allows the Town law enforcement agency to utilize hotlist and other specified information via License Plate Readers under the aegis of the DESPP Chief Systems Administrator (CSA).

VI. EFFECTIVE DATE, ADMINISTRATION AND TERMINATION

1. This MOU shall become effective when executed by both Parties and will continue in effect for one (1) year from the date of execution, at which point all parties shall discuss its future, including financial costs. This MOU may be modified at any time by written consent of both Parties.

2. This MOU may be terminated, with respect to either Party, at any time upon written notice of withdrawal to the other Party. The Party desiring to withdraw from this MOU will provide written notification to the other Party at least thirty (30) days prior to the withdrawal. Such notice will be the subject of immediate consultation by the Parties to decide upon the appropriate course of action. Notwithstanding any provisions in this MOU, DESPP, through a duly authorized employee, may terminate the Agreement whenever DESPP makes a written determination that such termination is in the best interests of the State.

FOR THE TOWN OF MARLBOROUGH

J. D Kehoe
JAY D. KEHOE
DIRECTOR OF PUBLIC SAFETY

11/18/2021
Date

FOR THE DEPARTMENT OF EMERGENCY SERVICES AND PUBLIC PROTECTION

J C R
James C. Rovella
Commissioner

11.29.2021
Date

1111 Country Club Road
Middletown, CT 06457
Phone: (860) 685-8150/Fax: (860) 685-8354
An Affirmative Action/Equal Opportunity Employer

DMV-MOU-MARLBOROUGH PD 2021-40-079

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE MARLBOROUGH POLICE DEPARTMENT
AND
THE DEPARTMENT OF MOTOR VEHICLES

THIS MEMORANDUM OF UNDERSTANDING (MOU) is made and entered into by and between the Marlborough Police Department, hereinafter referred to as "PD" and the State of Connecticut Department of Motor Vehicles, hereinafter referred to as "DMV", and is effective on the date of execution by the respective departments, as stated below.

PURPOSE: The PD and DMV agree that the intent and purpose of this MOU is to establish the terms, conditions and safeguards under which DMV will provide the PD with limited motor vehicle registration information from DMV files.

UNDERSTANDING: It is understood that DMV is authorized to issue and maintain the records of license plates for motor vehicles and the PD is a law enforcement department authorized to compile and maintain information concerning violations of laws of the state. The PD utilizes image processing technology known as License Plate Recognition (LPR) to identify vehicles by their license plates. The PD and DMV are permitted by their respective statutes and regulations to share record information and both departments recognize the critical need to protect public safety by obtaining the most accurate and up-to-date record information that is available, to enable appropriate and timely actions to be taken with respect to the registration status of a motor vehicle on public roads.

NOW, THEREFORE, the Director of the Marlborough Police Department and the Commissioner of Motor Vehicles hereby agree on behalf of their respective departments as follows:

1. DMV will provide the PD with access to a centrally located secure server to download a file of license plate numbers, vehicle descriptions (make, model and year) and corresponding registration class codes that have been identified in DMV records as having cancelled, suspended and expired registrations. The PD will update their LPR system with the electronic files of license plates as provided by DMV;

2. DMV will not provide any personal information, as defined by Section 14-10 of the Connecticut General Statutes, contained in these records;

3. All procedures, methods and requirements for the use of the LPR system have been developed solely by the PD and are described in Exhibit A, Marlborough Police Department License Plate Recognition Operational Procedures, attached hereto;

4. In accordance with Exhibit A, the PD will use the DMV information provided as an indicator only of a possible registration problem. The PD will confirm the license plate number, vehicle description, and administrative registration action on vehicles identified by the LPR through the Department of Emergency Services and Public Protection's Connecticut On-line Law Enforcement Communications Teleprocessing (COLLECT) system;

5. The PD agrees, represents, and warrants that it has obtained and will use the information furnished to it by the DMV for its own use and in connection with its LPR system only. Furthermore, the PD agrees that the information furnished by this MOU shall not be used, delivered, transmitted or otherwise conveyed to any other person, firm, partnership, corporation or any other entity, including other law enforcement entities; except where the PD has a written agreement with a vendor to perform the services contemplated in this agreement;

6. The PD agrees that the DMV shall not be responsible for any errors, omissions or discrepancies in the information furnished to the PD under this MOU;

7. DMV and the PD agree that each shall be responsible for all of its respective expenses and any liabilities that may be incurred with respect to any aspect of this MOU or performance hereunder. The PD agrees to defend, indemnify and save harmless the DMV from any and all claims and suits, and from liability of any kind whatsoever arising out of the PD's failure or alleged failure to follow the LPR procedures that it has developed, and that are specified in Exhibit A;

8. Amendments or additions to this MOU must be mutually agreed upon and shall be made only by written amendment, duly executed by both parties;

9. This MOU shall remain in effect until cancelled at any time by either party, without liability of any kind, upon (30) days' written notice to the other;

10. This MOU and the rights hereunder shall not be assigned by DMV or the PD;

11. The parties agree that this MOU and the interpretation of all its provisions shall be governed by the laws of the State of Connecticut;

12. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original and all of which together shall constitute one and the same instrument. Execution and delivery of this Agreement electronically is hereby deemed valid and effective; a signed PDF or electronic copy is hereby deemed an original for all purposes; and the parties fully intend that each may rely

upon such signature as being a true signature of the party's authorized officer or representative and deemed as due execution and delivery for all purposes whether or not hard copies of this Agreement were or are ever exchanged between them.

13. This MOU contains the entire agreement between the parties concerning the subject matter hereof, and supersedes any previous understandings, presentations, commitments or agreements, oral or written, relating hereto.

IN WITNESS THEREOF, the parties hereto have caused this MOU to be duly signed on the dates hereinafter stated.

Reviewed by: Terence Lavoie Porter-Lair Date: 11/17/21
DMV Legal Department

State of Connecticut
Department of Motor Vehicles

By: Sibongile Magubane Date: 11/17/2021
Sibongile Magubane
Commissioner

Marlborough Police Department

By: J D Kehoe Date: 10/14/2021
Jay D. Kehoe
Director of Public Safety

DMV-MOU-MARLBOROUGH PD 2021-40-079

EXHIBIT A

Marlborough Police Department
License Plate Recognition Operational Procedures

The Marlborough Police Department has developed and shall follow the procedures below, in regards to the DMV data, during its operation of their LPR:

- DMV-provided data shall be updated with the most current information available prior to use of the reader.
- Only officers trained in the operation of the LPR will be permitted to use the equipment.
- The LPR is to be used as a screening tool only.
- All hits discovered as a result of LPR operation shall be confirmed by other means prior to taking police action.
- DMV hits will be verified by means of a COLLECT[1]

[1] Department of Emergency Services and Public Protection's "Connecticut On Line Law Enforcement Communications Teleprocessing" system.

2456

flock safety

Automate investigative leads with a camera that sees like a detective

Flock Safety Falcon ™
Long Range ALPR Camera

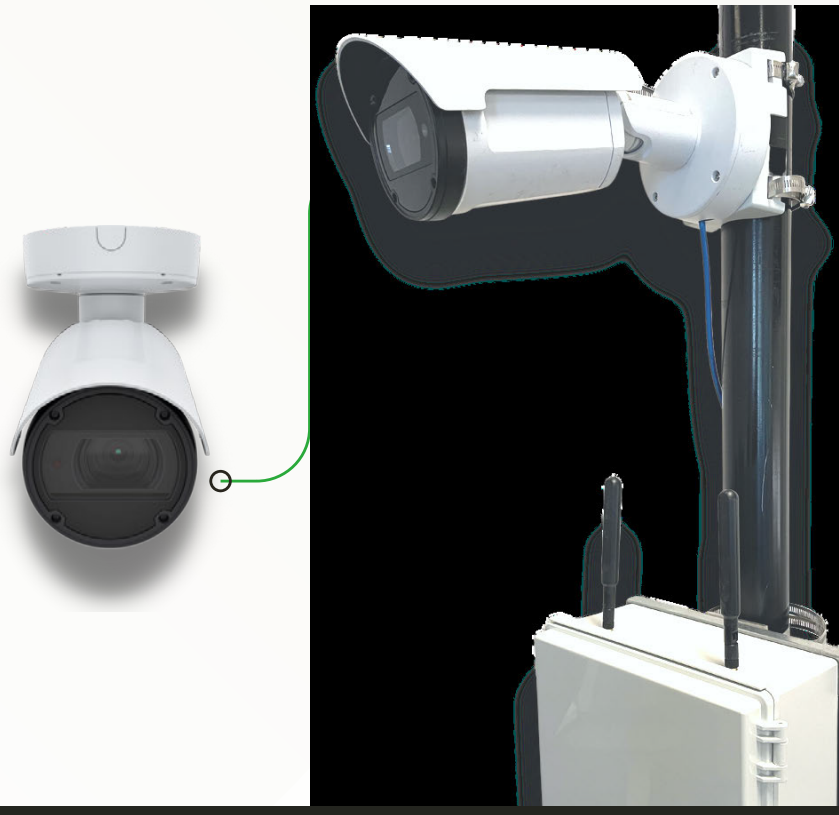
The Flock Safety Falcon is an affordable ALPR (automatic license plate reader) camera for law enforcement agencies who want to increase case clearance and eliminate crime. Unlike traditional ALPR, the Falcon can be deployed on any roadway and capture vehicles up to 150 feet away at 100 MPH. The Falcon's advanced computer vision uses Vehicle Fingerprint ™ technology to transform thousands of images into actionable evidence, even when a license plate isn't visible.

Not your average license plate reader

Install anywhere
With LTE connectivity, we can install the Falcon where it impacts crime the most.

No maintenance required
We install, maintain, and service your cameras for the life of your contract, all for one subscription price.

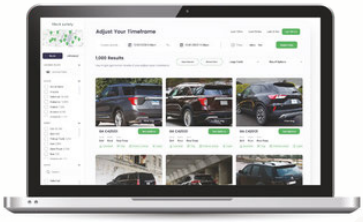
Vehicle Fingerprint Technology
Search images by vehicle type, make, color, license plate, and other unique features like bumper stickers, decals, and roof racks.



2457

Join over 2000 cities using Flock Safety to eliminate crime







Detect
objective evidence necessary to clear more cases

Decode
footage with machine learning to uncover investigative leads

Deliver
real-time alerts to dispatch, patrol, and detectives

Trustworthy technology that solves and prevents crime.

130%
More plate reads than the competition

30%
More accuracy than legacy LPR

120
Stolen plate and vehicle hits per hour

60%
Crime reduction in Cobb Co., GA

$1.1M
Recovered in stolen vehicles in Wichita, KS

"We are making significant arrests almost every single day."

- Lt. Casey Slaughter
Wichita Police Department



2458

Capture objective evidence 24/7 without the overtime pay



Identify vehicle body type, make, color, license plate (partial, missing, or covered plates), temporary plates, license plate state, and unique features like decals, bumper stickers, and accessories.

Use Cases

- Roadways: Capture evidence of vehicles on up to 3 lanes
- Speed: Capture vehicles traveling up to 100 mph
- Distance: Deployed up to 150 ft away from vehicles

Pole

- Existing Utility Pole/Structure
- 14' DOT Breakaway Pole
- Material: 6061 Aluminum
- Weight: 32 lbs

Power

- 120/240VAC 60Hz
- Fused Disconnect or Standard NEMA 5-15 Receptacle

Camera System

- Length: 14.2"
- Width: 5.8"
- Height: 5.8"
- Weight: 5.3 lbs
- 4K/10MP Image Sensor
- 20-86° HFOV

Compute System

- Length: 15.6"
- Width: 11.8"
- Height: 6.1"
- Weight: 15 lbs

Operational Conditions

- -40 to 60 C operating temperature
- IP66 Ingress rating

2459

U.S Department of Transportation

Federal Motor Carrier Safety Administration

Grant Agreement

1. RECIPIENT NAME AND ADDRESS
Transportation, Massachusetts Executive Office
10 Park Plz Ste 3170
Boston, MA 02116-3979

2. AGREEMENT NUMBER: 69A3601940337MHP0MA

3. AMENDMENT NO. 0

4. PROJECT PERFORMANCE PERIOD: FROM TO 09/30/2023

5. FEDERAL FUNDING PERIOD: FROM TO 09/30/2023

1A. IRS/VENDOR NO. 046002284

1B. DUNS NO. 824848659

6. ACTION New

7. CFDA#: 20.237

8. PROJECT TITLE
FY2019 HP-ITD Grant Program

TITLE	FEDERAL	NON-FEDERAL	TOTAL
9. PREVIOUS AGREEMENTS	0.00	0.00	0.00
10. THIS AGREEMENT	828,000.00	146,117.00	974,117.00
11. TOTAL AGREEMENT	828,000.00	146,117.00	974,117.00

12. INCORPORATED ATTACHMENTS
THIS AGREEMENT INCLUDES THE FOLLOWING ATTACHMENTS, INCORPORATED HEREIN AND MADE A PART HEREOF:

FMCSA Financial Assistance Agreement General Terms and Conditions, Recipient project narrative and indirect cost rate agreement (if applicable) are incorporated by reference unless/except as noted below.

13. STATUTORY AUTHORITY FOR GRANT/ COOPERATIVE AGREEMENT
49 U.S.C. §§ 31102(l); 31104 (2016), as amended by the FAST Act, Pub. L. No. 114-94, §§ 5101(a) and (c) (2015), Consolidated Appropriations Act 2019, Pub. L. No.116-6

14. REMARKS
See Award Conditions.

GRANTEE ACCEPTANCE		AGENCY APPROVAL	
15. NAME AND TITLE OF AUTHORIZED GRANTEE OFFICIAL Leslie Bestick Authorizing Official		17. NAME AND TITLE OF AUTHORIZED FMCSA OFFICIAL Rikita Jarrett	
16. SIGNATURE OF AUTHORIZED GRANTEE OFFICIAL Electronically Signed	16A. DATE 09/26/2019	18. SIGNATURE OF AUTHORIZED FMCSA OFFICIAL Electronically Signed	18A. DATE 09/26/2019

AGENCY USE ONLY

19. OBJECT CLASS CODE: 41000

20. ORGANIZATION CODE: M600000000

21. ACCOUNTING CLASSIFICATION CODES

DOCUMENT NUMBER	FUND	BY	BPAC	AMOUNT
FM-MHP-0485-19-01-00	17X05719MH	2019	0905710MHP	828,000.00

AWARD CONDITIONS

1. This Notice of Grant Award (NGA) awards the Recipient with the total award amount authorized in Block 11 to implement the FY 2019 High Priority Grant Program.

   The FMCSA approves the total project plan, line item budget and budget narrative as requested in the original application. The FY 2019 total recommended amount is $974,117. (Federal award = $828,000. / State match = $146,117).

   If the recipient is requesting indirect costs, the recipient may not request reimbursement for these costs until it has submitted a current approved indirect cost rate agreement to the FMCSA Division Office, and the GMO mailbox below:

   FMCSASECGMOHelpDesk@dot.gov

   The recipient and any sub-recipient must also comply with the applicable attached FMCSA general terms and conditions, which are incorporated into this NGA. Failure to comply with the attached terms and conditions and any additional provisions directly reflected in this NGA may result in enforcement actions as outlined in 2 CFR §§ 200.338 and 200.339.

AWARD ATTACHMENTS

Transportation, Massachusetts Executive Office FM-MHP-0485-19-01-00

1. Standard Terms and Conditions

FEDERAL MOTOR CARRIER SAFETY ADMINISTRATION
FINANCIAL ASSISTANCE AGREEMENT GENERAL TERMS AND CONDITIONS

Section 1. Grant Authority

a. Contract Authority.

The Federal Motor Carrier Safety Administration's (FMCSA) authorizing legislation, The Fixing America's Surface Transportation Act [FAST Act], Pub. L. No. 114-94, §5101 (2015) granted FMCSA contract authority. As codified in 49 U.S.C. §31104, the Secretary of Transportation's approval of the grant funds made available imposes a contractual obligation upon the United States for payment of the Government's share of costs in carrying out the grant objectives.

b. Lapse in Appropriations and/or Authorization.

Except in limited circumstances, the absence of FMCSA appropriations and/or authorization prevents the continuation of Federal supervision and support to the performance of a grant. In the absence of such supervision or support, the Recipient may only continue to proceed with its work if (1) the performance of such grant is not incurring obligations from the lapsed appropriations; (2) if continued grant management supervision or support is not critical to the Recipient's continued performance of the work; (3) and FMCSA has approved the continuation of such work. FMCSA will make such determinations in accordance with the Executive Office of the President, Office of Management and Budget, Memorandum "Planning for Agency Operations During a Lapse in Government Funding "(April 7, 2011), and any amendments or updated guidance thereto.

Section 2. Effective Date.

Recipient acknowledges that Federal funds are obligated on the effective date of the Grant Agreement. The effective date is the date that the Grant Agreement contains the authorized signatures of both parties to this agreement. Where the dates accompanying the signatures differ from party to party, the effective date of the Grant Agreement shall be the most recent of these dates.

Section 3. Electronic Signatures.

The Recipient understands that electronic signatures are binding. An electronic signature to the Grant Agreement commits the Recipient to these Provisions and Assurances, as well as all requirements denoted in Section 4.

Section 4. General Requirements.

a. Obligation of Recipient to Comply.

The Recipient understands that by signing the Grant Agreement, the Recipient is agreeing to carry out the approved project plan and the approved budget and to comply with all applicable Federal laws and requirements imposed by the FMCSA concerning special requirements of law, program requirements, and other administrative requirements. This includes, but is not limited to: (1) 49 U.S.C. chapters 311 and 313 (2016), as applicable and denoted in the Notice of Grant Agreement; (2) FAST Act, Pub. L. No. 114-94, §§ 5101 and 5104 (2015), as applicable and denoted in the Notice of Grant Agreement; (3) U.S. Department of Transportation (DOT) regulations; (4) the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (2 C.F.R. part 200); and (5) the Federal Grant and Cooperative Agreement Act of 1977.

For all Federal awards, compliance with statutory and national policy requirements also includes the provisions of the Federal Funding and Accountability Transparency Act (FFATA), which includes requirements on executive compensation, and also requirements implementing the Act for the non-Federal entity, codified at 2 C.F.R. part 25 and 2 C.F.R. part 170. See also statutory requirements for whistleblower protections at 10 U.S.C. §§ 2324 and 2409 and 41 U.S.C. § § 4304, 4310, and 4712.

b. Application of Federal, State, and Local Laws and Regulations.

i. Federal Laws.

The Recipient understands that Federal laws, regulations, policies, and related administrative practices applicable to this Agreement on the date the Agreement was executed may be modified from time to time. The Recipient agrees that the most recent of such Federal requirements will govern the administration of this Agreement at any particular time. Likewise, new Federal laws, regulations, policies and administrative practices may be established after the date the Agreement has been executed and may apply to this Agreement. To achieve compliance with changing Federal requirements, the Recipient agrees to include in all Subrecipient agreements and third-party contracts financed with FMCSA assistance, specific notice that Federal requirements may change and the changed requirements will apply to the Project as required. All limits or standards set forth in this Agreement to be observed in the performance of the Project are minimum requirements.

ii. State or Territorial Law and Local Law.

Except to the extent that a Federal statute or regulation preempts State or territorial law, nothing in this Agreement shall require the Recipient to observe or enforce compliance with any provision thereof, perform any other act, or do any other thing in contravention of any applicable State or territorial law;

however, if any of the provisions of this Agreement violate any applicable State or territorial law, or if compliance with the provisions of this Agreement would require the Recipient to violate any applicable State or territorial law, the Recipient agrees to notify the FMCSA immediately in writing in order that FMCSA and the Recipient may make appropriate arrangements to proceed with the Project as soon as possible.

c. Subrecipients.

State Recipients shall follow State law and procedures when awarding and administering subawards to local and Indian tribal governments including 2 C.F.R. § 200.317. All other non-federal entities, including Subrecipients of a State, will follow 2 C.F.R. § 200.318, General procurement standards, through § 200.326, Contract provision, as well as the Standards for Financial and Program Management, at §§ 200.300 through 200.309. Subrecipient means a non-Federal entity that receives a subaward from a pass-through entity to carry out part of a Federal program; but does not include an individual that is a beneficiary of such program. A Subrecipient may also be a recipient of other Federal awards directly from a Federal awarding agency.

d. Subawards.

Subaward means an award provided by a pass-through entity to a Subrecipient for the Subrecipient to carry out part of a Federal award received by the pass-through entity. It does not include payments to a contractor or payments to an individual that is a beneficiary of a Federal program. A subaward may be provided through any form of legal agreement, including an agreement that the pass-through entity considers a contract.

e. Pass-Through Entity.

Pass-through entity means a non-Federal entity that provides a subaward to a Subrecipient to carry out part of a Federal program. All Pass-Through Entities must comply fully with 2 C.F.R. §§ 200.330, 200.331, 200.332, and 200.505.

f. Prohibition Against Transferring An Award.

The Recipient is prohibited from transferring or subrogating their rights and responsibilities of the grant program and funds associated with that grant to another entity. Subrogation is when a non-federal entity substitutes another entity, not awarded the subject grant by FMCSA, to a lawful claim, demand, or right, so that that entity succeeds to the rights of the other in relation to the debt or claim, and its rights, remedies, or fund access. The act of subawarding to a Subrecipient is not considered as the subrogation of the Recipient's award.

Section 5. Internal Controls. The Recipient must:

a. Establish and maintain effective internal control over the Federal award that provides reasonable assurance that the non-Federal entity is managing the Federal award in compliance with Federal statutes, regulations, and the terms and conditions of the Federal award. These internal controls should be in compliance with guidance in "Standards for Internal Control in the Federal Government" issued by the Comptroller General of the United States and the "Internal Control Integrated Framework," issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO);

b. Comply with Federal statutes, regulations, and the terms and conditions of the Federal awards;

c. Evaluate and monitor the non-Federal entity's compliance with statute, regulations and the terms and conditions of Federal awards;

d. Take prompt action when instances of noncompliance are identified including noncompliance identified in audit findings; and

e. Take reasonable measures to safeguard protected personally identifiable information and other information the Federal awarding agency or pass-through entity designates as sensitive or the non-Federal entity considers sensitive consistent with applicable Federal, state and local laws regarding privacy and obligations of confidentiality.

Section 6. Ethics.

a. Written Code of Ethics.

The Recipient agrees to maintain a written code or standards of ethical conduct that shall govern the performance of its officers, employees, board members, or agents engaged in the award and administration of contracts supported by Federal funds. The code or standards shall provide that the Recipient's officers, employees, board members, or agents may neither solicit nor accept gratuities, favors or anything of monetary value from present or potential contractors, Subrecipients, or regulated entities. The Recipient may set minimum rules where the financial interest is not substantial or the gift is an unsolicited item of nominal intrinsic value. As permitted by State or local law or regulations, such code or standards shall provide for penalties, sanctions, or other disciplinary actions for violations by the Recipient's officers, employees, board members, or agents, or by contractors or·Subrecipients or their agents.

b. Personal Conflict of Interest.

The Recipient's code or standards must provide that no employee, officer, board member, or agent of the Recipient may participate in the selection, award, or administration of a contract supported by Federal funds if a real or apparent conflict of interest would be

involved. Such a conflict would arise when any of the parties set forth below has a financial or other interest in the firm selected for award:

i. The employee, officer, board member, or agent;
ii. Any member of his or her immediate family;
iii. His or her partner; or
iv. An organization that employs, is considering to employ, or is about to employ, any of the above.

c. Organizational Conflicts of Interest.

The Recipient's code or standards of conduct must include procedures for identifying and preventing real and apparent organizational conflicts of interests. An organizational conflict of interest exists when the nature of the work to be performed under a proposed third-party contract or subaward, may, without some restrictions on future activities, result in an unfair competitive advantage to the contractor or Subrecipient or impair the contractor's or Subrecipient's objectivity in performing the contract work.

Section 7. Hatch Act.

The Recipient agrees to comply, as applicable, with provisions of the Hatch Act (5 U.S.C. §§ 1501-1508 and 7321-7326), which limit the political activities of state or local employees whose principal employment is in connection with programs financed in whole or in part by loans or grants made by the United States or a Federal agency. The Hatch Act specifically exempts employees of educational institutions, and the Hatch is not applicable to private, nonprofit organizations unless the statutes through which the nonprofit organizations derive their federal funding contain a provision stating that the recipient organizations are deemed to be state or local government agencies for purposes of the Hatch Act. On December 19, 2012, Congress passed the Hatch Act Modernization Act of 2012 (the Act). The Act became effective on January 27, 2013. Now, only state, D.C., or local government employees whose salaries are paid for entirely by federal funds are prohibited from running for partisan office. All other state, D.C., and local employees, even if they are otherwise covered by Hatch Act restrictions are free under the Hatch Act to run for partisan office.

Section 8. Limitation on Use of Federal Funds for Lobbying for Grants in Excess of $100,000.

By signing this agreement, the Recipient declares that it is in compliance with 31 U.S.C. § 1352, which prohibits the use of federally appropriated funds to influence a Federal employee, officer, or Member of Congress in connection with the making or modification of any Federal grant, loan, contract, or cooperative agreement. Unless the payment of funds is otherwise reported to FMCSA, signing this agreement constitutes a declaration that no funds, including funds not federally appropriated, were used or agreed to be used to influence this grant.

Recipients of subawards in excess of $100,000 must make the same declarations to the Recipient. With respect to the payment of funds not federally appropriated by the Recipient and

Subrecipients, the Recipient must report to the FMCSA the name and address of each person paid or performing services for which payment is made, the amount paid, and the activity for which the person was paid.

Section 9. Contracting (Federal Standards).

The Recipient and Subrecipients agree to comply with the Procurement Standards requirements set forth at 2 C.F.R. §§ 200.317 through 200.326 inclusive, whichever may be applicable, and with applicable supplementary U.S. DOT or FMCSA directives or regulations. If determined necessary for proper Project administration, FMCSA reserves the right to review the Recipient's technical specifications and requirements.

Section 10. Notification Requirement.

With respect to any procurement for goods and services (including construction services) having an aggregate value of $500,000 or more, the Recipient agrees to:

a. Specify in any announcement of the awarding of the contract for such goods or services the amount of Federal funds that will be used to finance the acquisition; and

b. Express the said amount as a percentage of the total costs of the planned acquisition.

Section 11. Debarment and Suspension.

The Recipient agrees to obtain certifications on debarment and suspension from its third-party contractors and Subrecipients and otherwise comply with U.S. DOT regulations, Government-wide Debarment and Suspension (Non-procurement) and Government-wide Requirements for Drug-Free Workplace (Grants), 49 C.F.R. part 32. This action of certification shall take place for each federal year, regardless of prior certification completed for a Subrecipient or contractor.

Section 12. Notification of Third Party Contract or Subaward Disputes or Breaches.

The Recipient agrees to notify FMCSA of any current or prospective major dispute, breach, or litigation pertaining to any third-party contract or subaward. If the Recipient seeks to name FMCSA as a party to litigation for any reason, the Recipient agrees first to inform FMCSA before doing so. This provision applies to any type of litigation whatsoever, in any forum.

Section 13. Participation by Small Business Concerns Owned and Controlled by Socially and Economically Disadvantaged Individuals.

FMCSA encourages the Recipient to utilize small business concerns owned and controlled by socially and economically disadvantaged individuals (as that term is defined for other DOT agencies in 49 C.F.R. part 26) in carrying out the Project.

Section 14. Records Retention.

a. Requirement to Retain Records.

During the course of the Project and for three years after the final Federal financial report is submitted (form SF-425), the Recipient agrees to retain intact and to provide any data, documents, reports, records, contracts, and supporting materials relating to the Project as FMCSA may require. Reporting and record-keeping requirements are set forth in 2 C.F.R. § 200.333.

b. Access to Recipient and Subrecipient Records.

The Recipient, and related subrecipients, will give FMCSA, the Secretary of Transportation, the Comptroller General of the United States, or any of their duly authorized representatives, and, if appropriate the State, through any authorized representative, access to and the right to examine all records, books, papers or documents related to the award and will establish a proper accounting system in accordance with generally accepted accounting standards. Access requirements to records are set forth in 2 C.F.R. § 200.336.

Section 15. Audit and Inspection.

a. Inspector General Act of 1978.

Under the Inspector General Act of 1978, as amended, 5 U.S.C. App. 3 § 1 et seq., an audit of the award may be conducted at any time.

b. Single Audit Act Amendments of 1996.

The Recipient agrees to undergo the required financial and compliance audits in accordance with the Single Audit Act Amendments of 1996 and 2 C.F.R. § 200.501.

c. Other Audit Requirements.

A Recipient that is: (a) a State, local government or Indian tribal government, an institution of higher education or nonprofit organization agrees to comply with the audit requirements of 2 C.F.R. § 200.501, and any revision or supplement thereto; (c) a private for-profit organization agrees to comply with the audit requirements of 2 C.F.R. § 200.501(h).

It is imperative that Recipients submit required Single Audits within the time limits specified in the Circular. The Recipient agrees to submit the data collection form and copies of the reporting package required under the Single Audit Act Amendments of 1996 and 2 C.F.R. § 200.501 to:

The Federal Audit Clearinghouse Bureau of the Census
1201 East 10 Street,
Jefferson, IN 47132.

The Recipient agrees to obtain any other audits required by FMCSA. Project closeout will not alter the Recipient's audit responsibilities. Audit costs for Project administration and management are allowable under this Project to the extent authorized by 2 C.F.R. § 200.501.

The Recipient agrees to permit FMCSA, the Secretary of Transportation and the Comptroller General of the United States, or their authorized representatives, to inspect all Project work, materials, payrolls, and other data, and to audit the books, records, and accounts of the Recipient and its Subrecipients pertaining to the Project. The Recipient agrees to require each Subrecipient to permit the Secretary of Transportation and the Comptroller General of the United States, or their duly authorized representatives, to inspect all work, materials, payrolls, and other data and records involving that subaward, and to audit the books, records, and accounts involving that subaward as it affects the Project.

Section 16. Responsibility for Reporting Fraudulent Activity, Waste, and Abuse.

The Recipient understands that the Federal government shall pursue administrative, civil, or criminal action under a variety of statutes relating to fraud and making false statement or claims.

The Recipient is required to contact the DOT, the Office of Inspector General (OIG), if the Recipient becomes aware of the existence (or apparent existence) of fraudulent activity, waste, or abuse.

The OIG has authority within the DOT to conduct criminal investigations. The DOT OIG maintains a post office box and a toll-free hotline for receiving information from individuals concerning fraud, waste, or abuse under DOT grants and cooperative agreements. The hotline is available 24 hours a day, 7 days a week at https://www.oig.dot.gov/Hotline. The identity of the caller is kept confidential, and callers are not required to give their names.

Examples of fraud, waste, and abuse that should be reported include, but are not limited to, embezzlement, misuse, or misappropriation of grant funds or property, and false statements, whether by organizations or individuals. Other examples include, but not limited to, theft of grant funds for personal use; using funds for non-grant-related purposes; theft of federally owned property or property acquired or leased under a grant; charging inflated building rental fees for a building owned by the Recipient; submitting false financial reports; and submitting false financial data in bids submitted to the Recipient (for eventual payment under the grant).

Section 17. Budget and Finance.

The Recipient agrees to carry out Agreement activities and seek reimbursement in accordance with the Approved Project Budget after securing FMCSA written approval. The funding of items identified in the budget constitutes FMCSA 's authorization for the Recipient to incur these costs, if they are allowable, allocable, necessary, and reasonable. Furthermore, funds cannot be spent that violate any FMCSA policy or grants manual. Costs not specifically budgeted in this Agreement may be allowable if prior approval is not required and costs are

incurred consistently with the applicable cost principles.

Prior Approval means written permission provided by an FMCSA authorized official in advance of an act that would result in either (1) the obligation or expenditure of funds or (2) the performance or modification of an activity under the grant-supported project where such approval is required. Prior approval must be obtained in writing from the designated Grants Management Officer or FMCSA authorized official for the grant involved. Documentation of the approved budget on the Notice of Grant Award constitutes prior approval. Prior approval applies for the performance of activities and expenditure of funds as described in the grant application, unless otherwise restricted by the terms and conditions of the Agreement.

In accordance with 2 C.F.R. § 200.407 and § 200.308, the Recipient must obtain prior , written approval from FMCSA before making any revisions to the approved project budget and/or project plan: (1) extending the project period of the grant beyond the project period end date specified in the most recent revision of the Agreement; (2) that would require any transfer of funds between Standard Form (SF) 424A (direct-cost budget categories) cumulatively greater than ten percent of the total approved project budget; or (3) that require the addition of expenditures for items or services not approved in the original project plan. Examples include: increased cost of equipment purchased; subawarding, transferring or contracting out of any work under a Federal award not included in the original approved budget; or a first-time request to recover indirect costs.

The Recipient agrees to submit a request for prior approval no less than 30 days prior to the expiration of the Agreement. The FMCSA will not process requests for prior approval received less than 30 days from the Agreement expiration date. Within 30 calendar days from the date of the Recipient's request for prior approval, FMCSA will review the request and notify the Recipient whether the request has been approved. If the revision is still under consideration at the end of 30 calendar days, FMCSA will inform the Recipient in writing of the date when the Recipient may expect the decision.

The Recipient may, without prior approval from FMCSA, make any reasonable and necessary modification to the project budget if such deviations do not cumulatively exceed, or expect to exceed, ten percent of the total approved project amount and provided that such deviations only involve the transfer of funds between expenditure items, cost objectives or categories authorized by FMCSA in the currently approved budget. The Recipient agrees to notify FMCSA of this change.

The Recipient agrees to establish and maintain for the Project either a separate set of accounts or accounts within the framework of an established accounting system, in a manner consistent with 2 C.F.R. § 200.302. Consistent with the provisions of 2 C.F.R.§ 200.305, the Recipient agrees to record in the Project Account, and deposit in a financial institution all Project payments received by it from FMCSA pursuant to this Agreement and all other funds provided for, accruing to, or otherwise received because the Project (Project Funds). The Recipient is encouraged to use financial institutions owned at least 50 percent by minority group members.

All costs charged to the Project, including any approved services contributed by the Recipient

or others, shall be supported by properly executed payroll documents, time and attendance records, invoices, contracts, or vouchers describing in detail the nature and propriety of the charges. All match expenditures shall be supported by appropriate records. The Recipient also agrees to maintain accurate records of all Program Income derived from Project implementation. The Recipient agrees that all checks, payrolls, invoices, contracts, vouchers, orders, or other financial documents pertaining in whole or in part to the Project shall be clearly identified, readily accessible, and, to the extent feasible, kept separate from documents not pertaining to the Project.

Section 18. Payments.

a. Request by the Recipient for Payment.

The Recipient's request for payment of the Federal share of approved costs shall be made to FMCSA and will be acted upon by FMCSA as set forth in this section. Each payment made to the Recipient must be in compliance with Department of the Treasury regulations, "Rules and Procedures for Funds Transfers, 31 C.F.R. part 205. To receive a Federal assistance payment, the Recipient must:

i. Have demonstrated or certified that it has made a binding commitment of non-Federal funds, if applicable, adequate when combined with Federal payments, to cover all costs to be incurred under the Project to date. A Recipient required by Federal statute or this Agreement to provide contributory matching funds or a cost share agrees:

A. To refrain from requesting or obtaining Federal funds in excess of the amount justified by the contributory matching funds or cost share that has been provided; and

B. To refrain from taking any action that would cause the proportion of Federal funds made available to the Project at any time to exceed the percentage authorized under this Agreement. The requirement for contributory matching funds or cost share may be temporarily waived only to the extent expressly provided in writing by FMCSA.

ii. Have submitted to FMCSA all financial and progress reports required to date under this Agreement;

iii. Have identified the source(s) of financial assistance provided under this Project, if applicable, from which the payment is to be derived; and

iv. Have expended any earned Program Income before requesting any federal funds for reimbursement.

b. Delphi eInvoicing System for DOT Financial Assistance Awardees.

Subject to the requirements in 2 C.F.R. § 200.305, payments will be made after receipt of required FMC SA reporting forms and supporting documentation. Each payment request must be made electronically via the Delphi elnvoicing System.

The following are the procedures for accessing and utilizing the Delphi elnvoicing System.

i. Grant Recipient Requirements.

A. Recipient must have internet access to register and submit payment requests through the Delphi elnvoicing system.

B. Recipient must submit payment requests electronically and FMCSA must process payment requests electronically.

ii. System User Requirements.

A. Recipients should contact FMCSA to request access to the system. The FMCSA will provide the Recipient's name and email address to the DOT Financial Management Office. The DOT will then notify the Recipient to register for the system through an electronic invitation. The Recipient must complete online training prior to DOT giving system access.

B. The DOT will send the Recipient an email with an electronic form to verify the Recipient 's identity. The Recipient must complete the form, and present it to a Notary Public for verification. The Recipient will return the notarized form to:

DOT Enterprise Services Center
FAA Accounts Payable, AMZ-1 00
PO Box 25710
Oklahoma City, OK 73125.

C. The DOT will validate the form and email a user ID and password to the Recipient. The Recipient should contact the FMCSA grants management office with changes to their system information.

D. Note: Additional information, including access forms and training materials, can be found on the DOT elnvoicing website:
https://www.transportation.gov/cfo/delphi-einvoicing-system

E. Waivers.

DOT Financial Management officials may, in highly limited circumstances and on a case by case basis, waive the requirement to register and use the electronic grant payment system. Waiver request forms can be obtained on the DOT elnvoicing website https://www.transportation.gov/cfo/delphi-einvoicing-system or by contacting FMCSA.

Recipients must explain why they are unable to use or access the internet to register and enter payment requests.

c. Reimbursement Payment by FMCSA. If the reimbursement method is used, the Recipient agrees to:

i. Complete and submit Standard Form 3881, "Payment Information Form - ACH Payment Vendor Payment System," to FAA-ESC; and

ii. Complete and submit, on at least a quarterly basis, Standard Form 270, "Request for Advance or Reimbursement," to FMCSA.

iii. Possess and maintain a current DUNs number and entity registration with the System for Award Management (www.sam.gov).

Upon receipt of a payment request and adequate accompanying information (invoices in accordance with applicable cost principles), FMCSA will authorize payment by direct deposit provided the Recipient: (i) is in compliance with its obligations under this Agreement, (ii) has satisfied FMCSA that it needs the requested Federal funds during the requisition period, and (iii) is making adequate and timely progress toward Project completion. If all these circumstances are present, FMCSA may reimburse approved costs incurred by the Recipient up to the maxi mum amount of FMCSA's share of the total Project funding. FMCSA will employ a payment term of 20 days. The clock will start running for payment on receipt of the invoice by FMCSA's financial processor.

d. Other Payment Information.

The Recipient agrees to adhere to and impose on its Subrecipients all applicable foregoing "Payment by FMCSA" requirements of this Agreement. If the Recipient fails to adhere to the foregoing "Payment by FMCSA" requirements of this Agreement, FMCSA may revoke the portion of the Recipient's funds that has not been expended.

e. Effect of Program Income, Refunds, and Audit Recoveries on Payment.

In accordance with 2 C.F.R. § 200.305(b)(5) State, local government, nonprofit organizations and Indian tribunal Recipients and Subrecipients shall disburse program income, rebates, refunds, contract settlements, audit recoveries and interest earned on

such funds before requesting additional cash reimbursements.

f. Reimbursable Costs.

The Recipient's expenditures will be reimbursed only if they meet all requirements set forth below:

i. Conform with the Project description and the approved Project Budget and all other terms of this Agreement;

ii. Be necessary to accomplish the Project;

iii. Be reasonable for the goods or services purchased;

iv. Be actual net costs to the Recipient (i.e., the price paid minus any refunds, rebates, or other items of value received by the Recipient that have the effect of reducing the cost actually incurred);

v. Be incurred (and be for work performed) after the Federal Funding Period start date of this Agreement, unless specific prior authorization from FMCSA to the contrary is received in writing (pre-award costs);

vi. Unless permitted otherwise by Federal statute or regulation, conform with Federal guidelines or regulations and Federal cost principles as set forth below:

A. For Recipients that are governmental organizations, institutions of higher education, private non-profit organizations, the cost principles of 2 C.F.R. § 200, subpart E; and

B. For Recipients that are for-profit organizations, the standards of the Federal Acquisition Regulations, 48 C.F.R. part 31.2, "Contracts with Commercial Organizations" apply.

vii. Be satisfactorily documented; and

viii. Be treated uniformly and consistently as non-Federal funds under accounting principles and procedures approved and prescribed by FMCSA for the Recipient, and those approved or prescribed by the Recipient for its Subrecipients and contractors.

g. Indirect Costs.

If indirect costs are included in the approved budget, the Recipient may not request these costs for reimbursement absent a current approved indirect cost rate agreement submitted to the FMCSA Division Office, and included as part of the official grant record.

Indirect costs will not be reimbursed without documentation of an approved indirect cost rate from the Recipient's cognizant agency; however, a Recipient or Subrecipient that has never had a negotiated indirect cost rate may elect to charge a de minimis rate of 10% of modified total direct costs (MTDC) which may be used indefinitely, without documentation. If chosen, this methodology once elected must be used consistently for all Federal awards until such time as a non-Federal entity chooses to negotiate for a rate, which the non-Federal entity may apply to do at any time

As described in 2 C.F.R. § 200.403, factors affecting allowability of costs, costs must be consistently charged as either indirect or direct costs, but may not be double-charged or inconsistently charged as both. Except as provided above, if a Recipient intends to request reimbursement of indirect costs, the Recipient must submit the proper documentation before vouchers are submitted for reimbursement. The Recipient must indicate in its budget that it will be seeking indirect costs, and a placeholder indirect cost rate will suffice until an approved rate can be determined.

The Recipient must obtain prior approval through formal amendment in order to recover indirect costs at an approved rate higher than the place holder indirect cost rate if the cumulative amount of such transfer exceeds or is expected to exceed 10 percent of the total approved budget.

The Recipient may not request additional grant funds to recover indirect costs that it cannot recover by shifting funding from direct costs to indirect costs. After this Grant Agreement has been signed, any request for changes to the indirect cost rate will require an amendment and must be approved by formal amendment if the change to the indirect cost rate is a new rate or would cause the cumulative amount of a budget transfer to exceed 10 percent of the total approved budget.

The cognizant agency for indirect costs may allow for a one-time extension of the current indirect cost rate of up to four years without further negotiation of a federally approved indirect cost rate. If the cognizant agency permits any one-time extension, the Recipient is locked in with that indirect cost rate until the end of the approved extension.

h. Pre-Award Costs. A Recipient may be reimbursed for obligations incurred before the effective date of the award if:

i. The Recipient receives prior written approval from the FMCSA before the effective date of the grant agreement;

ii. The costs are necessary to conduct the project; and

iii. The costs would be allowable under the grant, if awarded.

If a specific expenditure would otherwise require prior approval before making the expenditure (i.e. pursuant to 2 C.F.R. § 200.407), then the Recipient must obtain FMCSA written approval before incurring the cost.

Recipient understands that the incurrence of pre-award costs in anticipation of an award is taken at the Recipient's risk and imposes no obligation on FMCSA to make the award or to increase the amount of the approved budget if (1) there is no award subsequently made;(2) an award is made for less than anticipated and is inadequate to cover the pre-award costs incurred; or (3) there are inadequate appropriations.

i. Disallowed Costs.

In determining the amount of Federal assistance FMCSA will provide, FMCSA will exclude:

i. Any Project costs incurred by the Recipient before the effective date of this Agreement, or amendment or modification thereof, whichever is later, unless otherwise permitted by Federal Law or regulation, or unless an authorized representative of FMCSA states in writing to the contrary;

ii. Any costs incurred by the Recipient that are not included in the latest approved Project Budget; and

iii. Any costs attributable to goods or services received under a contract or other arrangement that is required to be, but has not been, concurred with or approved in writing by FMCSA.

The Recipient agrees that reimbursement of any cost under the "Payment by FMCSA," part of this Agreement does not constitute a final FMCSA decision about the allowability of that cost and does not constitute a waiver of any violation by the Recipient of the terms of this Agreement. The Recipient understands that FMCSA will not make a final determination about the allowability of any cost until an audit of the Project has been completed. If FMCSA determines that the Recipient is not entitled to receive any part of the Federal funds requested, FMCSA will notify the Recipient stating the reasons thereof. Project closeout will not alter the Recipient's obligation to return any funds due to FMCSA as a result of later refunds, corrections, or other transactions. Nor will Project closeout alter FMCSA's right to disallow costs and recover funds based on a later audit or other review. Unless prohibited by law,

FMCSA may offset any Federal assistance funds to be made available under this Project as needed to satisfy any outstanding monetary claims that the Federal Government may have against the Recipient. Exceptions pertaining to disallowed costs will be assessed based on their applicability, as set forth in the applicable Federal cost principals or other written Federal guidance.

Section 19. Program Income.

Recipient agrees to comply with the regulations relating to program income, located at 2 C.F.R. §§ 200.305(b)(5) and 200.307 for State, local government, Indian tribunal recipients, and non-profit organizations, and their Subrecipients.

Program income means gross income earned by the Recipient, Subrecipient, or contractor under a grant that is directly generated by a grant-supported activity or earned because of the award during the award period. "During the grant period " is the time between the effective date of the award and the ending date of the award reflected in the final financial report.

Program income includes, but is not limited to, user charges or user fees, income from fees for services performed, the use or rental of real or personal property acquired under federally-funded projects, the sale of commodities or items fabricated under an award, license fees and royalties on patents and copyrights, and interest on loans made with award funds. Interest earned on advances of Federal funds is not program income. Except as otherwise provided in Federal awarding agency regulations or the terms and conditions of the award, program income does not include the receipt of principal on loans, rebates, credits, discounts, etc., or interest earned on any of them. Per 2 C.F.R. § 200.307 (c), Governmental revenues, taxes, special assessments, levies, fines, and other such revenues raised by a non-Federal entity are not program income unless the revenues are specifically identified in the Federal award or Federal awarding agency regulations as program income.

Recipients agree to use the Program income in accordance with 2 C.F.R. §§ 200.305(b)(5) 200.307 for State, local government, nonprofit organizations and Indian tribunal recipients and subrecipients.

Section 20. Reports.

a. Performance Progress Reports.

The Recipient will submit, at a minimum, quarterly performance progress reports and a final performance progress report at the completion of the award (within 90 days after) to the agency point of contact listed in the award document. Recipient must submit all performance progress report forms required by FMCSA. These reports will cover the period: January 1 -March 31, April 1-June 30, July 1- September 30, and October 1-December 31. The Recipient shall furnish one (1) copy of a quarterly performance progress report to the district office and respective Grant Manager, on or before the thirtieth (30th) calendar day of the month following the end of the quarter being reported. Each quarterly report shall set forth concise statements concerning activities relevant to the Project, and shall include, but not be limited to, the following:

i. An account of significant progress (findings, events, trends, etc.) made during the reporting period;

ii. A description of any technical and/or cost problem(s) encountered or anticipated

that will affect completion of the grant within the time and fiscal constraints as set forth in this Agreement, together with recommended solutions or corrective action plans (with dates) to such problems, or identification of specific action that is required by the FMCSA, or a statement that no problems were encountered;

iii. An outline of work and activities planned for the next reporting period; and

iv. A status update/resolution for all outstanding findings from program reviews and/or audits.

b. Quarterly Financial Status Reports.

The Recipient shall furnish one (1) copy of a quarterly financial status report to the division, and one (1) copy to the respective Grant Manager, on or before the thirtieth (30th) calendar day of the month following the end of the quarter being reported. The Recipient shall use SF-425, Federal Financial Report, to report the status of funds for all non-construction projects or programs. If the Recipient's accounting records are not normally kept on an accrual basis, the Recipient shall not be required to convert its accounting system, but shall develop such accrual information through an analysis of the documentation on hand. The Recipient shall certify to the expenditure of its proposed cost share for the period being reported, in the "Remarks" block.

Section 21. Non-Discrimination.

The Recipient will comply with all Federal authorities relating to nondiscrimination. These include, but are not limited to:

- Title VI of the Civil Rights Act of 1964 (42 U.S.C. § 2000d et seq., 78 Stat. 252), which prohibits discrimination on the basis of race, color, or national origin, as implemented by 49 C.F.R . § 21.1 et seq. and 49 C.F.R. § 303;
- Federal-Aid Highway Act of 1973, (23 U.S.C. § 324, et seq.), which prohibits discrimination on the basis of sex;
- Title IX of the Education Amendments of 1972, as amended, (20 U.S.C. § 1681 et seq.), which prohibits discrimination on the basis of sex in education programs or activities, as implemented by 49 C.F.R. § 25.1 et seq.;
- The Age Discrimination Act of 1975, as amended, (42 U.S.C. § 6101 et seq.), which prohibits discrimination on the basis of age;
- Section 504 of the Rehabilitation Act of 1973, (29 U.S.C. § 794 et seq.), as amended, which prohibits discrimination on the basis of disability and 49 C.F.R. part 27;
- Titles II and III of the Americans with Disabilities Act, which prohibit discrimination on the basis of disability in the operation of public entities, public and private transportation systems, places of public accommodation, and certain testing entities (42 U.S.C. §§ 12131 - 12189), as implemented by Department of Justice regulations at 28 C.F.R. parts 35 and 36, and Department of Transportation

regulations at 49 C.F.R. parts 37 and 38;
- The Civil Rights Restoration Act of 1987, (102 Stat. 28.), "which restore[d] the broad scope of coverage and to clarify the application of title IX of the Education Amendments of 1972, section 504 of the Rehabilitation Act of 1973, the Age Discrimination Act of 1975, and title VI of the Civil Rights Act of 1964.";
- Executive Order 12898, Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations, which prohibits discrimination against minority populations by discouraging programs, policies, and activities with disproportionately high and adverse human health or environmental effects on minority and low-income populations;
- Executive Order 13166, Improving Access to Services for Persons with Limited English Proficiency, and resulting Department of Transportation guidance, national origin discrimination includes discrimination because of limited English proficiency (LEP);
- Title VII of the Civil Rights Act of 1964, as amended, (42 U.S.C. § 2000e et seq., 78 Stat. 252), which prohibits discrimination in employment on basis of race, color, national origin, religion, or disability, as implemented by 29 C.F.R. § 1601.1, et seq.
- The Recipient also agrees to comply with the FMCSA Standard Title VI/Non-Discrimination Assurances (DOT Order No. 1050.2A).

Section 22. Executive Order on Equal Opportunity Related to Contracts.

The Recipient will comply with all Federal statutes and Executive Orders relating to Equal Employment Opportunity.

The Recipient agrees to incorporate in all contracts having a value of over $10,000, the provisions requiring compliance with Executive Order 11246, as amended, and implementing regulations of the United States Department of Labor at 41 C.F.R. part 60, the provisions of which, other than the standard EEO clause and applicable goals for employment of minorities and women, may be incorporated by reference.

The Recipient agrees to ensure that its contractors and subcontractors, regardless of tier, awarding contracts and/or issuing purchase orders for material, supplies, or equipment over $10,000 in value will incorporate the required EEO provisions in such contracts and purchase orders.

Section 23. Employment Policies.

The Recipient further agrees that its own employment policies and practices will be without discrimination based on race, color, religion, sex, national origin, disability or age; and that it has an affirmative action plan (AAP) consistent with the Uniform Guidelines on Employee Selection Procedures, 29 C.F.R. § 1607, and the Affirmative Action Guidelines, 29 C.F.R. § 1608. The applicant/Recipient shall provide the AAP to FMCSA for inspection or copy upon request.

Section 24. Property.

a. General.

In general, title to equipment and supplies acquired by a Recipient with DOT funds vests in the Recipient upon acquisition, subject to the property management requirements of 2 C.F.R. §§ 200.302(b)(4); 200.307(d); 200.310; 200.313; 200.316; and 200.344(4).

A Recipient that is a State, local, or Indian tribal governments, institutions of higher education, and non-profits agrees to comply with the property management standards detailed in 2 C.F.R. §§ 200.312 and 200.313, including any amendments thereto, and with other applicable Federal regulations and directives. A Recipient that is a for-profit entity agrees to comply with property management standards satisfactory to FMCSA.

b. Use of Project Property.

i. The State Recipient agrees to use Project property for the purpose for which it was acquired under the period of performance of the Grant. State Recipients acknowledge that the FMCSA may ensure that the purpose of the grant is being satisfied. State Recipients acknowledge that FMCSA may request a copy of the State statute and procedures in determining whether a State is in compliance with its own State procedures, and to assist the FMCSA in determining the allocability, reasonableness, and allowability of costs.

ii. The Non-State Recipient agrees to use Project property for appropriate Project purposes (which may include joint development purposes that generate program income, both during and after the award period, beginning on the effective date, and used to support public transportation activities) for the duration of the useful life of that property, as required by FMCSA. Should the Recipient unreasonably delay or fail to use Project property during the useful life of that property, the Recipient agrees that it may be required to return the entire amount of the Federal assistance expended on that property. The Non-State Recipient further agrees to notify FMCSA immediately when any Project property is withdrawn from Project use or when any Project property is used in a manner substantially different from the representations the Recipient has made in its Application or in the Project Description for the Grant Agreement or Cooperative Agreement for the Project.

c. Maintenance.

The State Recipient agrees to maintain Project property in accordance with State law and procedures.

The Non-State Recipient agrees to maintain Project property in good operating order, in compliance with any applicable Federal regulations or directives that may be issued.

d. Records.

The State Recipient agrees to maintain property records in accordance with State law and procedures. The Non-State Recipient agrees to keep satisfactory property records pertaining to the use of Project property, and submit to FMCSA upon request such information as may be required with this agreement.

e. Incidental Use.

Any incidental use of Project property will not exceed that permitted under applicable Federal laws, regulations, and directives.

f. Encumbrance of Project Property.

i. The State Recipient agrees to maintain satisfactory continuing control of Project property in accordance with State law and procedures. The State Recipient understands that an encumbrance of project property may not interfere with the purpose for which the equipment was purchased.

ii. The Non-State Recipient agrees to maintain satisfactory continuing control of Project property as follows:

A. Written Transactions.

The Non-State Recipient agrees that it will not execute any transfer of title, lease, lien, pledge, mortgage, encumbrance, third-party contract, subaward, grant anticipation note, alienation, innovative finance arrangement (such as a cross border lease, leveraged lease, or otherwise), or any other obligation pertaining to Project property, that in any way would affect the continuing Federal interest in that Project property.

B. Oral Transactions.

The Non-State Recipient agrees that it will not obligate itself in any manner to any third-party with respect to Project property.

C. Other Actions.

The Non-State Recipient agrees that it will not take any action adversely affecting the Federal interest in or impair the Recipient's continuing control of the use of Project property.

D. The Non-State Recipient agrees that no use under this section will interference with the purpose for which the equipment was purchased.

g. Transfer of Project Property.

i. The State Recipient agrees to transfer Project property in accordance with State law and procedures.

ii. The Non-State Recipient understands and agrees as follows:

A. Transfers.

The Non-State Recipient may transfer any Project property financed with Federal assistance authorized under 49 U.S.C. chapter 53 to a public body to be used for any public purpose with no further obligation to the Federal Government, provided the transfer is approved by the FMCSA Administrator and conforms with the requirements of 49 U.S.C. §§ 5334(h)(1) and (2). Any leasing or rental of equipment purchased by federal funds or state match/cost sharing, during the period of performance will considered program income and will be managed, expended, and reported per 2 C.F.R. § 200.307.

B. Federal Government Direction.

The Non-State Recipient agrees that the Federal Government may direct the disposition of, and even require the Recipient to transfer, title to any Project property financed with Federal assistance under the Grant Agreement or Cooperative Agreement.

h. Leasing Project Property to Another Party.

If the Non-State Recipient leases any Project property to another party, the Non- State Recipient agrees to retain ownership of the leased Project property, and assure that the lessee will use the Project property appropriately, either through a written lease between the Non-State Recipient and lessee, or another similar document.

Upon request by FMCSA, the Non-State Recipient agrees to provide a copy of any relevant documents. Any leasing or rental of equipment purchased by federal funds or state match/cost sharing, during the period of performance will be considered program income and will be managed, expended, and reported per 2 C.F.R. § 200.307.

i. Disposition of Project Property.

i. The State Recipient may use its own disposition procedures, provided that those procedures comply with the laws of that State.

ii. The Non-State Recipient agrees to dispose of Project property as follows:

A. With prior FMCSA approval, the Non-State Recipient may sell, transfer, or lease Project property and use the proceeds to reduce the gross project cost of other eligible capital public transportation projects to the extent permitted by 49 U.S.C. §5334(h)(4). The Non-State Recipient also agrees that FMCSA may establish the useful life of Project property, and that it will use Project property continuously and appropriately throughout the useful life of that property.

B. Project Property with Expired Useful Life. When the useful life of Project property has expired, the Non-State Recipient agrees to comply with FMCSA's disposition requirements.

C. Project Property Prematurely Withdrawn from Use. For Project property withdrawn from appropriate use before its useful life has expired, the Recipient agrees as follows:

D. Notification Requirement. The Non-State Recipient agrees to notify FMCSA immediately when any Project property is prematurely withdrawn from appropriate use, whether by planned withdrawal, misuse, or casualty loss.

E. Calculating the Fair Market Value of Prematurely Withdrawn Project Property. The Non-State Recipient agrees that the Federal Government retains a Federal interest in the fair market value of Project property prematurely withdrawn from appropriate use. The amount of the Federal interest in the Project property shall be determined by the ratio of the Federal assistance awarded for the property to the actual cost of the property. The Non-State Recipient agrees that the fair market value of Project property prematurely withdrawn from use will be calculated as follows:

1. **Equipment and Supplies.** The Non-State Recipient agrees that the fair market value of Project equipment and supplies shall be calculated by straight-line depreciation of that property, based on the useful life of the equipment or supplies as established or approved by FMCSA. Information on straight line depreciation may be found in the Internal Revenue Code. The fair market value of Project equipment and supplies shall be the value immediately before the occurrence prompting the withdrawal of the equipment or supplies from appropriate use. In the case of Project equipment or supplies lost or damaged by fire, casualty, or natural disaster, the fair market value shall be calculated on the basis of the condition of that equipment or supplies immediately before the fire, casualty, or natural disaster, irrespective of the extent of insurance coverage.

2. **Real Property**. The Non-State Recipient agrees that the fair market value of real property shall be determined either by competent appraisal based on an appropriate date approved by the Federal Government, as provided by 49 C.F.R. part 24, or by straight line depreciation, whichever is greater.

3. **Exceptional Circumstances.** The Non-State Recipient agrees that the Federal Government may require the use of another method to determine the fair market value of Project property. In unusual circumstances, the Non-State Recipient may request that another reasonable valuation method be used including, but not limited to, accelerated depreciation, comparable sales, or established market values. In determining whether to approve such a request, the Federal Government may consider any action taken, omission made, or unfortunate occurrence suffered by the Non-State Recipient with respect to the preservation of Project property withdrawn from appropriate use.

j. Financial Obligations to the Federal Government.

The Recipient agrees to remit to the Federal Government the Federal interest in the fair market value of any Project property prematurely withdrawn from appropriate use. In the case of fire, casualty, or natural disaster, the Recipient may fulfill its obligations to remit the Federal interest by either:

Investing an amount equal to the remaining Federal interest in like-kind property that is eligible for assistance within the scope of the Project that provided Federal assistance for the Project property prematurely withdrawn from use; or

Returning to the Federal Government an amount equal to the remaining Federal interest in the withdrawn Project property.

k. Insurance Proceeds.

If the Recipient receives insurance proceeds as a result of damage or destruction to the Project property, the Recipient agrees to:

i. Apply those insurance proceeds to the cost of replacing the damaged or destroyed Project property taken out of service, or

ii. Return to the Federal Government an amount equal to the remaining Federal interest in the damaged or destroyed Project property.

l. Transportation of Hazardous Materials.

The Recipient agrees to comply with applicable requirements of U.S. Pipeline and Hazardous Materials Safety Administration regulations, "Shippers - General Requirements for Shipments and Packagings," 49 C.F.R. part 173, in connection with the transportation of any hazardous materials.

m. Misused or Damaged Project Property.

If any damage to Project property results from abuse or misuse occurring with the Recipient's knowledge and consent, the Recipient agrees to restore the Project property to its original condition or refund the value of the Federal interest in that property, as the Federal Government may require.

n. Responsibilities after Project Closeout.

The Recipient agrees that Project closeout by FMCSA will not change the Recipient's Project property management responsibilities as stated in these Grant Provisions and Assurances, and as may be set forth in subsequent Federal laws, regulations, and directives, except to the extent the Federal Government determines otherwise in writing.

Section 25. Davis-Bacon Act Requirements.

The Recipient agrees to comply, as applicable, with the provisions of the Davis Bacon Act (40 U.S.C. § 3145 and 18 U.S.C. § 874), and the Contract Work Hours and Safety Standards Act (40 U.S.C. §§ 3701 et seq.) regarding labor standards for federally-assisted construction sub-agreements.

Section 26. Environmental Requirements.

The Recipient agrees to comply, as applicable, with environmental standards which may be prescribed pursuant to the following: (a) institution of environmental quality control measures under the National Environmental Policy Act of 1969 (P.L. 91-190) and Executive Order (EO) 11514; (b) notification of violating facilities pursuant to EO 11738; (c) protection of wetlands pursuant to EO 11990; (d) evaluation of flood hazards in floodplains in accordance with EO 11988; (e) assurance of project consistency with the approved State management program developed under the Coastal Zone Management Act of 1972 (16 U.S.C. §§ 1451 et seq.); (f) conformity of Federal actions to State (Clean Air) Implementation Plans under Section 176(c) of the Clean Air Act of 1955, as amended (42 U.S.C. §§ 7401 et seq.); (g) protection of underground sources of drinking water under the Safe Drinking Water Act of 1974, as amended (P.L. 93-523); and, (h) protection of endangered species under the Endangered Species Act of 1973, as amended (P.L. 93-205).

Section 27. Government Rights (Unlimited).

FMCSA shall have unlimited rights for the benefit of the Government in all other work developed in the performance of this Agreement, including the right to use same on any other Government work without additional cost to FMCSA. The rights to any inventions made by a Recipient under an FMCSA financial assistance award are determined by the Bayh-Dole Act, Pub. L. 96-517, as amended, and codified in 35 U.S.C. § 200, et seq., except as otherwise provided by law.

a. Patent Rights.

If any invention, improvement, or discovery of the Recipient or any of its third-party contractors is conceived or first actually reduced to practice in the course of or under this Project, and that invention, improvement, or discovery is patentable under the laws of the United States of America or any foreign country, the Recipient agrees to notify FMCSA immediately and provide a detailed report. The rights and responsibilities of the Recipient, third-party contractors and FMCSA with respect to such invention, improvement, or discovery will be determined in accordance with applicable Federal laws, regulations, policies, and any waiver thereof.

If the Recipient secures a patent with respect to any invention, improvement, or discovery of the Recipient or any of its third-party contractors conceived or first actually reduced to practice in the course of or under this Project, the Recipient agrees to grant to FMCSA a royalty-free, non- exclusive, and irrevocable license to use and to authorize others to use the patented device or process for Federal Government purposes.

The Recipient agrees to include the requirements of the "Patent Rights" section of this Agreement in its third-party contracts for planning, research, development, or demonstration under the Project.

b. Data Rights.

The term "subject data" used in this section means recorded information, whether or not copyrighted, that is developed, delivered, or specified to be delivered under this Agreement. The term includes graphic or pictorial delineations in media such as drawings or photographs; text in specifications or related performance or design-type documents; machine forms such as punched cards, magnetic tape, or computer memory printouts; and information retained in computer memory. Examples include, but are not limited to: computer software, engineering drawings and associated lists, specifications, standards, process sheets, manuals, technical reports, catalog item identifications, and related information. The term does not include financial reports, cost analyses, and similar information incidental to Project administration. The following restrictions apply to all subject data first produced in the performance of this Agreement:

i. Except for its own internal use, the Recipient may neither publish or reproduce such data in whole or in part, or in any manner or form, nor may

the Recipient authorize others to do so, without the written consent of FMCSA, until such time as FMCSA may have either released or approved the release of such data to the public.

ii. As authorized by 2 C.F.R. § 200.315(b), FMCSA reserves a royalty-free, non-exclusive and irrevocable license to reproduce, publish or otherwise use, and to authorize others to use, for Federal Government purposes:

A. Any work developed under a grant, cooperative agreement, sub-grant, sub-agreement, or third-party contract, irrespective of whether or not a copyright has been obtained; and

B. Any rights of copyright to which a Recipient, Subrecipient, or a third-party contractor purchases ownership with Federal assistance.

iii. When FMCSA provides assistance to a Recipient for a Project involving planning, research, or development of a system, program, document, enforcement concept, or any other activity provided for in the terms of this grant, it is generally FMCSA's intent to increase the body of knowledge, rather than to limit the benefits of the Project to those parties that have participated therein. Therefore, unless FMCSA determines otherwise, the Recipient understands and agrees that, in addition to the rights set forth in preceding portions of this section of this Agreement, FMCSA may make available to any FMCSA Recipient, Subrecipient, third-party contractor, or third-party subcontractor, either FMCSA's license in the copyright to the "subject data" derived under this Agreement or a copy of the "subject data" first produced under this Agreement. In the event that such a Project which is the subject of this Agreement is not completed, for any reason whatsoever, all data developed under that Project shall become subject data as defined herein and shall be delivered as FMCSA may direct.

iv. Unless prohibited by State law, the Recipient agrees to indemnify, save and hold harmless FMCSA, its officers, agents, and employees acting within the scope of their official duties against any liability, including costs and expenses, resulting from any willful or intentional violation by the Recipient of proprietary rights, copyrights, or right of privacy, arising out of the publication, translation, reproduction, delivery, use, or disposition of any data furnished under this Agreement. The Recipient shall not be required to indemnify FMCSA for any such liability arising out of the wrongful acts of employees or agents of FMCSA.

v. Nothing contained in this section on rights in data, shall imply a license to FMCSA under any patent or be construed as affecting the scope of any license or other right otherwise granted to FMCSA under any patent.

vi. The requirements of this section of this Agreement do not apply to material furnished to the Recipient by FMCSA and incorporated in the work carried out

under this Agreement, provided that such incorporated material is identified by the Recipient at the time of delivery of such work.

vii. Unless FMCSA determines otherwise, the Recipient agrees to include the requirements of this section of this Agreement in its third-party contracts for planning, research, development, or demonstration under the Project.

c. Acknowledgment or Support and Disclaimer.

i. An acknowledgment of FMCSA support and a disclaimer must appear in any Recipient publication, whether copyrighted or not, based on or developed under the Agreement, in the following terms:

"This material is based upon work supported by the Federal Motor Carrier Safety Administration under a grant/cooperative agreement/subaward, dated (fill-in appropriate identification of grant/cooperative agreement);"

ii. All Recipient publications must also contain the following:

"Any opinions, findings, and conclusions or recommendations expressed this publication are those of the author(s) and do not necessarily reflect the view of the Federal Motor Carrier Safety Administration and/or the U.S. Department of Transportation."

iii. The Recipient agrees to cause to be erected at the site of any construction, and maintain during construction, signs satisfactory to FMCSA identifying the Project and indicating that FMCSA is participating in the development of the Project.

Section 28. Drug Free Workplace.

By signing this agreement, the Recipient certifies that it is in compliance with the Drug-Free Workplace Act (41 U.S.C. §§ 701 et seq.) and implementing regulations (49 C.F.R. part 32), which require, in part, that Recipients prohibit drug use in the workplace, notify the FMCSA of employee convictions for violations of criminal drug laws occurring in the workplace, and take appropriate personnel action against a convicted employee or require the employee to participate in a drug abuse assistance program.

Section 29. Background Screening.

FMCSA reserves the right to perform individual background screening on key individuals of organizational units associated with the application at the effective date and at another interval thereafter for the life of the award. If in performance of a grant award requires Recipient organization personnel to have unsupervised physical access to a federally controlled facility for

more than 180 days or access to a Federal information system, such personnel must undergo the personal identity verification credential process under Homeland Security Presidential Directive 12.

Section 30. Site Visits.

FMCSA, through its authorized representatives, has the right, at all reasonable times, to make site visits to review Project accomplishments and management control systems and to provide such technical assistance as may be required. If any site visit is made by FMCSA on the premises of the Recipient, Subrecipient, or contractor under this Agreement, the Recipient shall provide and shall require its Subrecipients or contractors to provide, all reasonable facilities and assistance for the safety and convenience of FMCSA representatives in the performance of their duties. All site visits and evaluations shall be performed in such a manner as will not unduly delay work being conducted by the Recipient, Subrecipient, or subcontractor.

Section 31. Liability.

The Recipient acknowledges it is responsible for any act or omission of Recipient or Subrecipient, its officers, contractors, employees, or members, participants, agents, representatives, as appropriate, arising out of or in any way connected to activities authorized pursuant to this Agreement.

The Recipient acknowledges that FMCSA is not responsible for any act or omission of Recipient or Subrecipient, its officers, contractors, employees, or members, participants, agents, representatives, as appropriate, arising out of or in any way connected to activities authorized pursuant to this Agreement. This provision shall survive the expiration or termination of this Agreement.

Section 32. Right of FMCSA to Terminate Agreement.

a. General Right to Suspend or Terminate Assistance Agreement.

Upon written notice, the Recipient agrees that FMCSA may suspend or terminate all or part of the financial assistance provided herein if the Recipient has violated the terms of the Grant Agreement or these Provisions and Assurances, or if FMCSA determines that the purposes of the statute under which the Project is authorized would not be adequately served by continuation of Federal financial assistance for the Project. Any failure to make reasonable progress on the Project or other violation of this Agreement that significantly endangers substantial performance of the Project shall provide sufficient grounds for FMCSA to terminate this Agreement. The Recipient agrees to give the Federal Motor Carrier Safety Administration at least 90 days' notice of its intention to terminate this agreement.

b. Financial Obligations of the Government.

In general, termination of any financial assistance under this Agreement will not

invalidate obligations properly incurred by the Recipient and concurred by FMCSA before the termination date; to the extent those correctly accrued obligations cannot be cancelled.

However, if FMCSA determines that the Recipient has willfully misused Federal assistance funds by failing to make adequate progress, failing to make reasonable use of the Project property, facilities, or equipment, or failing to adhere to the terms of this Agreement, meet required match/cost sharing or maintenance of effort (MOE) levels, FMCSA reserves the right to require the Recipient to refund the entire amount of FMCSA funds provided under this Agreement or any lesser amount as may be determined by FMCSA.

c. De-obligation of Funds.

FMCSA reserves the right to unilaterally de-obligate any remaining grant or cooperative agreement funds due to the time elapsed since the effective date, lack of payment vouchers from the Recipient, lack of plans to expend funds based on this grant, failure to provide quarterly progress reports, or other such determination made by FMCSA. If FMCSA takes action to deobligate funds, a grant amendment/modification must be in place.

Section 33. Project Completion, Settlement, and Closeout.

a. Project Completion.

Within 90 days of the Project completion date or termination by FMCSA, the Recipient agrees to submit a final SF-425, Federal Financial Report, a certification or summary of Project expenses, and third-party au it reports, as applicable.

b. Remittance of Excess Payments.

If FMCSA has made payments to the Recipient in excess of the total amount of FMCSA Federal funding due to cover accumulated expenses, the Recipient agrees to promptly remit that excess and interest as may be required by the "Payment by FMCSA" section of this Attachment.

c. Project Closeout.

Project closeout, as defined in 2 C.F.R. § 200.16, occurs when all required Project work and all administrative procedures described in 2 C.F.R. § 200.343, as applicable, have been completed, and when FMCSA notifies the Recipient and forwards the final Federal assistance payment, or when FMCSA acknowledges the Recipient's remittance of the proper refund amount. Project closeout shall not invalidate any continuing obligations imposed by allowable, allocable, and reasonable costs on the Recipient by this Agreement that supports the project plan(s) or by the FMCSA's final notification or acknowledgment, if it occurs within the period of performance.

Section 34. Severability.

If any provision of this Agreement is held invalid, all remaining provisions of this Agreement shall continue in full force and effect to the extent not inconsistent with such holding.

Section 35. Entire Agreement and Amendments.

This Agreement constitutes the entire agreement between the parties. All prior discussions and understandings concerning such scope and subject matter are superseded by this Agreement.

Any modification not specifically permitted by this agreement requires an Amendment. These modifications may be made only in writing, signed by each party's authorized representative, and specifically referred to as an Amendment to this Agreement. Electronic signatures are binding. However, retroactive modifications to the project plan(s) or any aspects of the budget will not be approved.

Section 36. Use of Information Obtained.

Information obtained under this agreement may only be used by the Recipient to accomplish the project plan under this agreement.

Any information obtained or exchanged between FMCSA and the grant Recipient, to carry out each party 's responsibility under this agreement and project plan, shall not be released by the Recipient to any third-party without the written permission of FMCSA.

Recipient shall ensure that all its employees authorized to access FMCSA data and information systems sign and submit information technology user agreements provided by FMCSA.

Section 37. Miscellaneous Provisions.

a. Prohibition on Human Trafficking.

The Recipient agrees to comply, as applicable, with the provisions of Section 7104(g) of the Trafficking Victims Protection Act of 2000, 22 U.S.C. § 7104 as amended.

b. Wild and Scenic Rivers Act of 1968.

The Recipient agrees to comply, as applicable, with the Wild and Scenic Rivers Act of 1968 (16 U.S.C. §§1271 et seq.) related to protecting components or potential components of the national wild and scenic rivers system.

c. Fly America Act.

The Recipient shall comply with the provisions of the Fly America Act, 49 U.S.C. § 401 18.

d. Criminal and Prohibited Activities.

The Recipient will adhere to the Program Fraud Civil Remedies Act, 31 U.S.C. § 3801- 3812, which provides for the imposition of civil penalties against persons who make false, fictitious, or fraudulent claims to the Federal Government for money. Recipient will also adhere to the False Statements Act, 18 U.S.C. §§ 287 and 1001 which provides that whoever makes or presents any false, fictitious or fraudulent statements, representation, or claims against the United States shall be subject to imprisonment of not more than 5 years and shall be subject to a fine in the amount provided by 18 U.S.C. § 287. Recipient shall also adhere to the False Claims Act, 31 U.S.C. § 3729, which provides that suits under this act can be brought by the Government or a person on behalf of the Government, for false claims under the Federal assistance programs. Recipient shall also adhere to the Copeland "Anti-Kickback" Act, 18 U.S.C. § 874 and 40 U.S.C. § 3145, which prohibits a person or organization engaged in a federally supported project from enticing an employee working on the project from giving up a part of his compensation under an employment contract.

Section 38. Laptop Encryption.

All laptops used by Recipients, Subrecipients, and contractors in carrying out the Recipient 's project plan, which contain FMCSA-related data, including sensitive information and Personally Identifiable Information (PII), must be encrypted to the same standards utilized by FMCSA. The FMCSA encryptions standards prescribe whole disk encryption (FOE), which requires software or hardware to encrypt all data on a disk, including the partition tables, whole physical disk, master boot record, and available files. FMCSA requires that each Recipient who utilizes FMCSA sensitive information or PII complete installation of FOE on all laptop computers as soon as practicable, but no later than thirty (30) days from the execution of this agreement and prior to using the laptop to access FMCSA data systems or store FMCSA related data.

Section 39. Adaptability to Climate Changes.

If the grant is to be used to place equipment or temporary facilities, modify structures, or to alter existing infrastructure, the recipient is required to assess the ability for the equipment, modifications, or alterations to withstand current and future climatic conditions, including potential changes in climatic conditions. The recipient shall use the best-available peer reviewed studies and science to determine the potential climatic conditions the equipment, modifications or alterations may experience over the life-cycle of the equipment, modification or alteration funded by the grant. The recipient can rely on existing Federal Highway Administration suggestions or guidelines for placing infrastructure, or on other federally-issued guidance on assessing potential impacts of climate change.

Section 40. Commercial Vehicle Information Systems and Networks (CVISN) provisions.

The following provisions apply where applicable.

a. Compliance with the National ITS Architecture.

The recipient will ensure that Innovative Technology Deployment (ITD) activities, such as hardware procurement, software and system development, infrastructure modifications, etc., are consistent with the National ITS and commercial motor vehicle information and systems architectures and available standards and promote interoperability and efficiency to the extent practicable and required by law.

b. Interoperability.

For implementing ITD capabilities, the recipient will complete interoperability tests and ensure architectural conformance throughout the life of the project. Perform pairwise and end-to-end tests to demonstrate conformance with the standards and interoperability, verify that interfaces between selected products/systems meet the applicable standards, verify dataflow and data usage among the products/systems.

c. Independent Evaluation.

The FMCSA may conduct an independent evaluation of the effectiveness of the project in achieving Federal and State program goals. The independent evaluation will be conducted using existing Federal resources. Participants of projects that are selected for independent evaluations shall cooperate with the independent evaluators and participate in evaluation planning and progress review meetings to ensure a mutually acceptable, successful implementation of the independent evaluation. The FMCSA may contract with one or more independent evaluation contractor(s) to evaluate the projects.

d. Dedicated Short-Range Communications.

If applicable, the State shall also require that its contractors only install Dedicated Short Range Communications (DSRC) equipment that is interoperable and compatible at layers 1 and 2 of the Open Systems Interconnect Reference Model with equipment in operation on the North American Preclearance and Safety System and the Heavy Vehicle Electronic License Plate Inc.'s PrePass™ System deployments as well as the International Border Crossing Operational Tests, based upon on ASTM Draft 6, dated February 23, 1996.

Section 41. Federal Funding Accountability and Transparency Act.

The Federal Funding Accountability and Transparency Act (FFATA) of 2006 (Public Law 109-282) requires for each Federal award of $25,000 or more that OMB create a searchable, no cost, publicly accessible website(http://usaspending.gov/) that includes basic

information about the recipient and the project being funded. The Government Funding Transparency Act of 2008 (Public Law 110-252) amended FFATA, requiring recipients to report certain information about themselves and their first tier Subrecipient awards obligated as of October 1, 2010. Prime grant recipients/awardees of new non-Recovery Act federally funded grants and cooperative agreements of $25,000 or more awarded on or after October 1, 2010 are subject to FFATA reporting, sub-award reporting requirements and executive compensation reporting requirements as outlined in the Office of Management and Budgets guidance issued August 27, 2010. The prime awardee is required to file a FFATA sub-award report by the end of the month following the month in which the prime recipient awards any sub-grant greater than or equal to $25,000.

Section 42. Executive Order 13513.

Executive Order 13513 (E.O. 13513) requires each Federal agency to encourage contractors, subcontractors, and grant and cooperative agreement recipients and subrecipients to adopt and enforce policies that ban text messaging while driving company-owned or -rented vehicles or Government Owned Vehicles, or while driving Personally Owned Vehicles when on official Government business or when performing any work for or on behalf of the Government. To further the requirement of encouraging such policies, the FMCSA encourages recipients to consider new rules and programs, reevaluate existing programs to prohibit text messaging while driving, and conduct education, awareness, and other outreach for employees about the risks associated with texting while driving. These initiatives should encourage voluntary compliance with the recipient agency's text messaging policy while off duty. For the purposes of these Grant Provisions and Assurances and pursuant to E.O. 13513, the following definitions apply:

> "Texting" or "Text Messaging" means reading from or entering data into any handheld or other electronic device, including for the purpose of SMS texting, e-mailing, instant messaging, obtaining navigational information, or engaging in any other form of electronic data retrieval or electronic data communication.
>
> "Driving" means operating a motor vehicle on an active roadway with the motor running, including while temporarily stationary because of traffic, a traffic light or stop sign, or otherwise. It does not include operating a motor vehicle with or without the motor running when one has pulled over to the side of, or off, an active roadway and has halted in a location where one can safely remain stationary.

Section 43. Certification.

The Recipient certifies that the statements it made in the grant application are true and correct, and Recipient understands that any false statements made as part of these certifications can be prosecuted.



CERTIFICATE OF TRAINING

THIS CERTIFICATE IS PROUDLY PRESENTED TO

Andrew Franquiz

FOR THE SUCCESSFUL COMPLETION OF

VIGILANT VEHICLEMANAGER 101

on Jul 04, 2023

1 Hour

PRESENTED BY

Marcia Broderick

Marcia Broderick
Director, Customer Training and Development

MOTOROLA SOLUTIONS



CERTIFICATE OF TRAINING

THIS CERTIFICATE IS PROUDLY PRESENTED TO

Andrew Franquiz

FOR THE SUCCESSFUL COMPLETION OF

VIGILANT VEHICLEMANAGER INTRODUCTION & USER ACCOUNT MANAGEMENT

on Jul 04, 2023
30 Minutes

PRESENTED BY

Marcia Broderick

Marcia Broderick
Director, Customer Training and Development

MOTOROLA SOLUTIONS

2497

Massachusetts Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Grant Division

QUARTERLY FINANCIAL REPORT

Agency/Contractor Name:	Massachusetts State Police	**Date:**	Tuesday, July 11, 2023
Project Name:	Fusion Center Maturation	**E-mail:**	jeff.ly@pol.state.ma.us
Grant Program & FFY:	FSHSP20CFC 8000-4692 FFY2020	**Telephone:**	508-988-7081
Reported by:	Jeff Ly	**FAX:**	508-820-2165

Report Number	Reporting Period	Year	Report Due
Quarter ___	July 1st – September 30th	2023	October 15th
Quarter ___	October 1st – December 31st	2023	January 15th
Quarter ___	January 1st – March 31st	2024	April 15th
Quarter _X_	April 1st – June 30th	2023	July 15th

SUMMARY OF COSTS

Expense Category	Amended Budget	Expended This Quarter	Expended to Date	Obligated to Date	Balance	% Remaining
Salary	$48,570.00	$0.00	$48,570.00	$0.00	0.00	0%
Fringe	$20,640.79	$0.00	$20,640.79	$0.00	0.00	0%
Indirect	$8,524.05	$0.00	$8,524.05	$0.00	0.00	0%
Consultants/Contracts	$75,615.00	$0.00	$75,615.00	$0.00	0.00	0%
Travel	$4,526.47	$0.00	$5,226.47	$0.00	(700.00)	0%
Equipment	$407,000.00	$398,526.69	$398,526.69	$5,693.96	2,779.35	0%
Supplies	$0.00	$0.00	$0.00	$0.00	0.00	0%
Overtime	$0.00	$0.00	$0.00	$0.00	0.00	0%
Other (software, registrations, seminars)	$185,123.69	$160,442.91	$184,162.91	$0.00	960.78	0%
TOTAL	**$750,000.00**	**$558,969.60**	**$741,265.91**	**$5,693.96**	**$3,040.13**	0%

Reports must be submitted for every full or partial calendar quarter during the grant period regardless of spending activity.

Please send this report along with the Quarterly Financial Detail and Quarterly Progress Reports to:

Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720A
Boston, MA 02116
ATTN: Vicky Mboka-Boyer *via email*

Authorized Signature (Blue ink please)

Date

Kellie Gray

Print Name

Executive Office of Public Safety

Quarterly Financial Report (Detail for Expenditures)

Quarter Reporting Period (Choose From Cell Below)
4/1-6/30

Year Reporting Period (Choose From Cell Below)
2023

FSHSP20CFC -

Salary:Please List all Employees charged to grant along with either: hours and rate, if paid hourly; or amount paid to employee for period from federal funds and a brief description, if salaried

Employee Name	Hrs/Unit	Rate/Amt	Description		Total
					-
					-
				Sub-Total:	**$0.00**

Fringe: Fringe costs must go by Federally approved rate, and base amount should easily be identified from this detailed report.

Employee Name	Approved Rate	Total dollars	Pay period		Total
				Sub-Total:	**$0.00**

Indirect: Indirect Rate must be a federally Negotiated and approved rate, and base amount should easily be identified from this detailed report.

Employee/Contracted Employee Name	Approved Rate	Total dollars			Total
					$ -
				Sub-Total:	$ -

Consultants/Contracts: Please list Name of Consultant or Entity contract is with, hours and rate of contract and a brief description. If total costs for quarter for any single contract exceed $5K, please provide invoices for

Company/Name	Hours	Rate	Description		Total
					-
					-
				Sub-Total:	**$0.00**

Travel: Please list each employee, cost of travel, description/purpose of travel, and the guidelines followed for reimbursement (Local, State, or Federal). Please include all receipts.

Employee Name	Cost	Guidelines	Purpose/Description	Total	Receipt Y/N
				Sub-Total:	$0.00

Piece of equipment	Unit Cost	Quantity	Description of Equipment	Total	Receipt
12x Trailers	[redacted]	[redacted]	12 Battery Mounted solar trailers	$249,606.00	
20x Neology Cameras & Kits			20 ALPR Neology Cameras & Kits	$148,920.69	
				Sub-Total:	$398,526.69

Supplies: Please list supplies and computation basis for reimbursement request.

Item	Cost		Basis for Computation	Total	
				Sub-Total:	$0.00

Overtime

Employee Name	Hrs/Unit	Rate/Amt	Description	Total	
				Sub-Total:	$0.00

Other: Please list Item and Basis for Computation.

Item	Cost	Qty	Basis for Computation	Total	Receipt
9x Analyst Notebooks	17,826.99	9	9 i2 Analyst Notebook & Software Subscription	$160,442.91	
				Sub-Total:	$160,442.91

Total

Total:*	$558,969.60

FSHSP20CFC	lumber if Appli	DESCRIPTION	Dates of Travel	B01	B02	B05	B08	B10	C98 - Contracted	Total
Grunewald, Brady	T-9G-22	Foundations of Intelligence Analysis Training course in NYC	09/12 -09/17	$ 1,974.46		$ 550 00				$2,524.46
Neville, John		National Association of Bunco Investigators in Prussia PA	10/18 -10/20	$ 689.40		$ 150 00				$839.40
Stelmat, Jason		Privacy Training to GHQ	10/21, 10/14, 06/24						$33.75	$33.75
		TOTAL FOR 10/1/2021 -12/31/2021		**$ 2,663.86**	**$ -**	**$ 700.00**	**$ -**	**$ -**	**$33.75**	$3,397.61

FSHSP20CFC	lumber if Appli	DESCRIPTION	Dates of Travel	B01	B02	B05	B08	B10	C98 - Contracted	Total
Andrew Franquiz	T-28G-22		02/6/22 -02/12/22	$ 1,598.08	$ 175.21					$1,773.29
Neville, John										$0.00
		TOTAL FOR 01/01/2022 -03/31/2022		**$1,598.08**	**$175.21**	**$0.00**	**$0.00**	**$0.00**	**$0.00**	**$1,773.29**

FSHSP20CFC	lumber if Appli	DESCRIPTION	Dates of Travel	B01	B02	B05	B08	B10	C98 - Contracted	Total
		TOTAL FOR 04/01/2022 - 06/30/22							**$0.00**	**$0.00**
FSHSP20CFC	**lumber if Appli**	**DESCRIPTION**	**Dates of Travel**	**B01**	**B02**	**B05**	**B08**	**B10**	**C98 - Contracted**	**Total**
Paul Upton		In-state Mileage To/From Training at MPTC and Beverly PD			$ 55.57					$55.57
		TOTAL FOR 07/01/2022 - 09/30/22			**$ 55.57**	**$ -**	**$ -**	**$ -**	**$0.00**	**$55.57**

Note: B05 registrations are posted to "other" category

TOTAL BB	$ 5,192.72
TOTAL CC	$ 33.75
	$ 5,226.47

2500

FSHSP20CFC
8000-4692

fiscal year	department	doc code	cash_expense amount	service_from date	service_to date	appropriation	object	object_name	vendor_customer code	legal name	program	acceptance date
2023	POL	EFT	(5,094.00)	06-Apr-23	06-Apr-23	80004692	K10	Law Enforcement & Security Equipment	VC0000506451	BAIN COR INC	FSHSP20CFC	14-Apr-23
2023	POL	EFT	254 700.00	06-Apr-23	06-Apr-23	80004692	K10	Law Enforcement & Security Equipment	VC0000506451	BAIN COR INC	FSHSP20CFC	14-Apr-23
2023	POL	EFT	160,442.91	23-Mar-23	23-Mar-23	80004692	U12	Information Tech (IT) cloud services	VC6000239916	INSIGHT PUBLIC	FSHSP20CFC	04-May-23
2023	POL	EFT	(3,039.20)	03-May-23	03-May-23	80004692	U07	Information Technology (IT) Equipment	VC0000500765	BAY STATE ALAF	FSHSP20CFC	12-May-23
2023	POL	EFT	151 959.89	03-May-23	03-May-23	80004692	U07	Information Technology (IT) Equipment	VC0000500765	BAY STATE ALAF	FSHSP20CFC	12-May-23

Total 6/30/2023 Expenditures 558,969.60

FSHSP20CFC
8000-4692

fiscal year	department	doc code	cash_expense amount	service_from date	service_to date	appropriation	object	object_name	vendor_customer code	legal name	program	acceptance date
2022	POL	PRLNP	2,025.00	03-Aug-21	03-Aug-21	80004692	A01	Salaries: Inclusive			FSHSP20CFC	03-Aug-21
2022	POL	PRLNP	3 000.00	03-Aug-21	03-Aug-21	80004692	C23	Management Business Professionals & Ad			FSHSP20CFC	03-Aug-21
2022	POL	PRLNP	1,830.00	17-Aug-21	17-Aug-21	80004692	A01	Salaries: Inclusive			FSHSP20CFC	17-Aug-21
2022	POL	PRLNP	3,000.00	17-Aug-21	17-Aug-21	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	17-Aug-21
2022	POL	PRLNP	2 610.00	31-Aug-21	31-Aug-21	80004692	A01	Salaries: Inclusive			FSHSP20CFC	31-Aug-21
2022	POL	PRLNP	3,000.00	31-Aug-21	31-Aug-21	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	31-Aug-21
2022	POL	CA	127.36			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	11-Sep-21
2022	POL	CA	177.30			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	11-Sep-21
2022	POL	CA	1,134.61			80004692	E16	Indirect Cost Recoupment			FSHSP20CFC	11-Sep-21
2022	POL	CA	2,421.79			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	11-Sep-21
2022	POL	PRLNP	1 680.00	14-Sep-21	14-Sep-21	80004692	A01	Salaries: Inclusive			FSHSP20CFC	14-Sep-21
2022	POL	PRLNP	3,000.00	14-Sep-21	14-Sep-21	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	14-Sep-21
2022	POL	PRADJ	580.00	15-Sep-21	15-Sep-21	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	15-Sep-21
2022	POL	PRADJ	3,035.00	15-Sep-21	15-Sep-21	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	15-Sep-21
2022	POL	PRLNP	1,950.00	28-Sep-21	28-Sep-21	80004692	A01	Salaries: Inclusive			FSHSP20CFC	28-Sep-21
2022	POL	PRLNP	3,000.00	28-Sep-21	28-Sep-21	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	28-Sep-21
2022	POL	CA	71.51			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	10-Oct-21
2022	POL	CA	189.42			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	10-Oct-21
2022	POL	CA	637.07			80004692	E16	Indirect Cost Recoupment			FSHSP20CFC	10-Oct-21
2022	POL	CA	1,359.80			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	10-Oct-21
2022	POL	PRLNP	550.00	12-Oct-21	12-Oct-21	80004692	B05	Conference, Training, Registration and Me			FSHSP20CFC	12-Oct-21
2022	POL	PRLNP	1,974.46	12-Oct-21	12-Oct-21	80004692	B01	Other Out Of State Travel - INCLUSIVE: AIR			FSHSP20CFC	12-Oct-21
2022	POL	PRLNP	2,520.00	12-Oct-21	12-Oct-21	80004692	A01	Salaries: Inclusive			FSHSP20CFC	12-Oct-21
2022	POL	PRLNP	3 000.00	12-Oct-21	12-Oct-21	80004692	C23	Management Business Professionals & Ad			FSHSP20CFC	12-Oct-21
2022	POL	PRLNP	2,850.00	26-Oct-21	26-Oct-21	80004692	A01	Salaries: Inclusive			FSHSP20CFC	26-Oct-21
2022	POL	PRLNP	3,000.00	26-Oct-21	26-Oct-21	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	26-Oct-21
2022	POL	CA	105.79			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	07-Nov-21
2022	POL	CA	118.20			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	07-Nov-21
2022	POL	CA	942.44			80004692	E16	Indirect Cost Recoupment			FSHSP20CFC	07-Nov-21
2022	POL	CA	2 011.60			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	07-Nov-21
2022	POL	PRLNP	2,670.00	09-Nov-21	09-Nov-21	80004692	A01	Salaries: Inclusive			FSHSP20CFC	09-Nov-21
2022	POL	PRLNP	3,000.00	09-Nov-21	09-Nov-21	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	09-Nov-21
2022	POL	PRLNP	2 685.00	23-Nov-21	23-Nov-21	80004692	A01	Salaries: Inclusive			FSHSP20CFC	23-Nov-21
2022	POL	PRLNP	3,000.00	23-Nov-21	23-Nov-21	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	23-Nov-21
2022	POL	CA	105.49			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	04-Dec-21
2022	POL	CA	118.20			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	04-Dec-21
2022	POL	CA	939.80			80004692	E16	Indirect Cost Recoupment			FSHSP20CFC	04-Dec-21
2022	POL	CA	2,005.98			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	04-Dec-21
2022	POL	PRLNP	150.00	07-Dec-21	07-Dec-21	80004692	B05	Conference, Training, Registration and Me			FSHSP20CFC	07-Dec-21
2022	POL	PRLNP	689.40	07-Dec-21	07-Dec-21	80004692	B01	Other Out Of State Travel - INCLUSIVE: AIR			FSHSP20CFC	07-Dec-21
2022	POL	PRLNP	2,040.00	07-Dec-21	07-Dec-21	80004692	A01	Salaries: Inclusive			FSHSP20CFC	07-Dec-21
2022	POL	PRLNP	3,000.00	07-Dec-21	07-Dec-21	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	07-Dec-21
2022	POL	PRLNP	7.59	21-Dec-21	21-Dec-21	80004692	C98	Reimb Travel/Other Expenses CC Special C			FSHSP20CFC	21-Dec-21
2022	POL	PRLNP	26.16	21-Dec-21	21-Dec-21	80004692	C98	Reimb Travel/Other Expenses CC Special C			FSHSP20CFC	21-Dec-21
2022	POL	PRLNP	1,935.00	21-Dec-21	21-Dec-21	80004692	A01	Salaries: Inclusive			FSHSP20CFC	21-Dec-21
2022	POL	PRLNP	3 000.00	21-Dec-21	21-Dec-21	80004692	C23	Management Business Professionals & Ad			FSHSP20CFC	21-Dec-21
2022	POL	PRLNP	1,035.00	04-Jan-22	04-Jan-22	80004692	A01	Salaries: Inclusive			FSHSP20CFC	04-Jan-22
2022	POL	PRLNP	3,000.00	04-Jan-22	04-Jan-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	04-Jan-22
2022	POL	CA	78.31			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	15-Jan-22
2022	POL	CA	118.20			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	15-Jan-22
2022	POL	CA	697.61			80004692	E16	Indirect Cost Recoupment			FSHSP20CFC	15-Jan-22
2022	POL	CA	1 489.04			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	15-Jan-22
2022	POL	PRLNP	2,055.00	18-Jan-22	18-Jan-22	80004692	A01	Salaries: Inclusive			FSHSP20CFC	18-Jan-22
2022	POL	PRLNP	3,000.00	18-Jan-22	18-Jan-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	18-Jan-22
2022	POL	PRLNP	2 595.00	01-Feb-22	01-Feb-22	80004692	A01	Salaries: Inclusive			FSHSP20CFC	01-Feb-22
2022	POL	PRLNP	3,000.00	01-Feb-22	01-Feb-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	01-Feb-22
2022	POL	CA	60.87			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	05-Feb-22
2022	POL	CA	118.20			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	05-Feb-22
2022	POL	CA	542.30			80004692	E16	Indirect Cost Recoupment			FSHSP20CFC	05-Feb-22
2022	POL	CA	1,157.51			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	05-Feb-22
2022	POL	PRLNP	1,920.00	15-Feb-22	15-Feb-22	80004692	A01	Salaries: Inclusive			FSHSP20CFC	15-Feb-22
2022	POL	PRLNP	3,000.00	15-Feb-22	15-Feb-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	15-Feb-22
2022	POL	PRLNP	175.21	01-Mar-22	01-Mar-22	80004692	B02	In-State Travel			FSHSP20CFC	01-Mar-22
2022	POL	PRLNP	550.00	01-Mar-22	01-Mar-22	80004692	B05	Conference, Training, Registration and Me			FSHSP20CFC	01-Mar-22
2022	POL	PRLNP	1,260.00	01-Mar-22	01-Mar-22	80004692	A01	Salaries: Inclusive			FSHSP20CFC	01-Mar-22
2022	POL	PRLNP	1,598.08	01-Mar-22	01-Mar-22	80004692	B01	Other Out Of State Travel - INCLUSIVE: AIR			FSHSP20CFC	01-Mar-22
2022	POL	PRLNP	3,000.00	01-Mar-22	01-Mar-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	01-Mar-22
2022	POL	CA	88.95			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	05-Mar-22
2022	POL	CA	118.20			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	05-Mar-22
2022	POL	CA	792.38			80004692	E16	Indirect Cost Recoupment			FSHSP20CFC	05-Mar-22
2022	POL	CA	1 691.32			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	05-Mar-22
2022	POL	EFT	136.00	13-Jan-22	30-Jun-22	80004692	U10	Information Tech (IT) Equipment Mainten	VC6000227588	SHI INTERNATIC	FSHSP20CFC	11-Mar-22
2022	POL	PRLNP	2,250.00	15-Mar-22	15-Mar-22	80004692	A01	Salaries: Inclusive			FSHSP20CFC	15-Mar-22
2022	POL	PRLNP	3 000.00	15-Mar-22	15-Mar-22	80004692	C23	Management Business Professionals & Ad			FSHSP20CFC	15-Mar-22
2022	POL	PRLNP	154.00	29-Mar-22	29-Mar-22	80004692	B05	Conference, Training, Registration and Me			FSHSP20CFC	29-Mar-22
2022	POL	PRLNP	3,000.00	29-Mar-22	29-Mar-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	29-Mar-22
2022	POL	PRLNP	3 000.00	29-Mar-22	29-Mar-22	80004692	A01	Salaries: Inclusive			FSHSP20CFC	29-Mar-22
2022	POL	CA	128.25			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	09-Apr-22
2022	POL	CA	177.30			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	09-Apr-22
2022	POL	CA	1,142.51			80004692	E16	Indirect Cost Recoupment			FSHSP20CFC	09-Apr-22
2022	POL	CA	2,438.65			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	09-Apr-22
2022	POL	PRLNP	2,820.00	12-Apr-22	12-Apr-22	80004692	A01	Salaries: Inclusive			FSHSP20CFC	12-Apr-22
2022	POL	PRLNP	3,000.00	12-Apr-22	12-Apr-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	12-Apr-22

2022	POL	PRLNP	2 325.00	26-Apr-22	26-Apr-22	80004692	A01	Salaries: Inclusive			FSHSP20CFC	26-Apr-22
2022	POL	PRLNP	3,000.00	26-Apr-22	26-Apr-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	26-Apr-22
2022	POL	CA	101.36			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	07-May-22
2022	POL	CA	118.20			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	07-May-22
2022	POL	CA	902.95			80004692	E16	Indirect Cost Recoupment			FSHSP20CFC	07-May-22
2022	POL	CA	1,927.32			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	07-May-22
2022	POL	PRLNP	1,905.00	10-May-22	10-May-22	80004692	A01	Salaries: Inclusive			FSHSP20CFC	10-May-22
2022	POL	PRLNP	3,000.00	10-May-22	10-May-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	10-May-22
2022	POL	PRLNP	2,130.00	24-May-22	24-May-22	80004692	A01	Salaries: Inclusive			FSHSP20CFC	24-May-22
2022	POL	PRLNP	3,000.00	24-May-22	24-May-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	24-May-22
2022	POL	PRLNP	480.00	07-Jun-22	07-Jun-22	80004692	A01	Salaries: Inclusive			FSHSP20CFC	07-Jun-22
2022	POL	PRLNP	3,000.00	07-Jun-22	07-Jun-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	07-Jun-22
2022	POL	CA	79.49			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	11-Jun-22
2022	POL	CA	118.20			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	11-Jun-22
2022	POL	CA	708.14			80004692	E16	Indirect Cost Recoupment			FSHSP20CFC	11-Jun-22
2022	POL	CA	1,511.51			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	11-Jun-22
2022	POL	EFT	22 880.00	09-May-22	09-May-22	80004692	U03	Software & Information Technology Licens	VC6000227588	SHI INTERNATIC	FSHSP20CFC	13-Jun-22
2022	POL	PRLNP	3,000.00	21-Jun-22	21-Jun-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	21-Jun-22
2022	POL	PRLNP	55.57	06-Jul-22	06-Jul-22	80004692	B02	In-State Travel			FSHSP20CFC	06-Jul-22
2022	POL	CA	9.46			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	09-Jul-22
2022	POL	CA	84.24			80004692	E16	Indirect Cost Recoupment			FSHSP20CFC	09-Jul-22
2022	POL	CA	118.20			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	09-Jul-22
2022	POL	CA	179.81			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	09-Jul-22
2023	POL	EFT	(5,094.00)	06-Apr-23	06-Apr-23	80004692	K10	Law Enforcement & Security Equipment	VC0000506451	BAIN COR INC	FSHSP20CFC	14-Apr-23
2023	POL	EFT	254,700.00	06-Apr-23	06-Apr-23	80004692	K10	Law Enforcement & Security Equipment	VC0000506451	BAIN COR INC	FSHSP20CFC	14-Apr-23
2023	POL	EFT	160 442.91	23-Mar-23	23-Mar-23	80004692	U12	Information Tech (IT) cloud services	VC6000239916	INSIGHT PUBLIC	FSHSP20CFC	04-May-23
2023	POL	EFT	(3,039.20)	03-May-23	03-May-23	80004692	U07	Information Technology (IT) Equipment	VC0000500765	BAY STATE ALAF	FSHSP20CFC	12-May-23
2023	POL	EFT	151,959.89	03-May-23	03-May-23	80004692	U07	Information Technology (IT) Equipment	VC0000500765	BAY STATE ALAF	FSHSP20CFC	12-May-23

Total Expenditures	741,265.91



2503

Reimbursable Grants: Level 2

Menu

	Department	Major Program	Program	Funding Profile	Funding Priority	Funding Line	Obligation Ceiling	Pre Encumbered	Encumbered	Total Expenses
✓	POL	HSG2	FSHSP20CFC	FEDGRT	1	1	$750,000.00	$0.00	$5,693.96	$741,265.91

First Prev Next Last

Search

Expense Actuals

Pre Encumbered :	$0.00	Obligation Ceiling :	$750,000.00
Encumbered :	$5,693.96	Expenditure Ceiling :	$750,000.00
Advances :	$0.00	Uncommitted :	$3,040.13
Accrued Expenses :	$0.00	Unexpended :	$8,734.09
Cash Expenses :	$741,265.91	Back End Splits :	$0.00
Total Expenses :	$741,265.91		
Charges :	$0.00		

Revenue Actuals

Unbilled Earned Revenue :	$0.00	Collected Earned Revenue :	$741,265.91
Billed Earned Revenue :	$0.00	Collected Unearned/Deferred Revenue :	$0.00
		Total Revenue :	$741,265.91
		Revenue Credits :	$0.00

Budgetary Amounts

Beginning Balance :	$0.00	Revenue Beginning Balance :	$0.00
Awarded :	$750,000.00	Original Revenue Budget :	$0.00
Amendments :	$0.00	Revenue Amendments :	$0.00
Transfer Out :	$0.00	Current Revenue Budget :	$0.00
Transfer In :	$0.00	Unrecognized Revenue :	($741,265.91)
Current Modified Budget :	$750,000.00	Revenue Balance Forward :	$0.00
Balance Forward :	$0.00		

General Information

Department :	POL	Name :	FFY20 SHSP
Major Program :	HSG2	Start Date :	12/15/2020
Program :	FSHSP20CFC	End Date :	
Funding Profile :	FEDGRT	Parent Dept :	105
Funding Priority :	1	Description :	EXECUTIVE OFFICE OF PUBLIC SAFETY & HOMELAND SECURITY
Funding Line :	1	Legal Cite :	
		Active :	☑

Top

Modified Budget Line Controls Previous Level

Pymt Request-CommodityBased(PRC) **Dept:** POL **ID:** PVPOL721423102BAIN01 **Ver.:** 1 **Function:** New **Phase:** Draft Final RIA

Modified by polajβ , 04/12/2023

Vendor **Total Lines:** 1 **Vendor Line:** 1 **Vendor Customer:** VC0000506451 **Legal Name:** BAIN COR INC

	Vendor Line	Vendor Customer	Legal Name	Line Amount
	1	VC0000506451	BAIN COR INC	254700.00

From 1 to 1 Total: 1 FSHSP20CFC unit #7214 8000-4692

General Information

Vendor Customer: VC0000506451
Legal Name: BAIN COR INC
Alias/DBA:
Address Code: AD001
Address 1: 105 TAMARACK LN
Address 2:
City: ABINGTON
State: Massachusetts
Zip Code: 02351-4026
Country: USA
County:

Vendor Contact ID:
Vendor Contact Name: SUZANNE MARKS
Vendor Contact Phone: 339-987-5525
Vendor Contact Phone Ext.:
Vendor Contact Email:
Fax:
Fax Extension:
Web Address http://:
Taxpayer ID Number:
Taxpayer ID Type:
Merchant ID:
Tax Profile:
Received Service From Date:
Received Service To Date:

Disbursement Options

Disbursement Type: EFT
Disbursement Format: CTX
Scheduled Payment Date: 04/15/2023
Disbursement Priority: 99
Single Payment: ☐
Pay Third Party: ☐
On-line Disbursement Rqst: ☐
EFT Status: Eligible for EFT

Handling Code:
Disbursement Category: 100

Invoice Information

Invoice Doc Code:
Invoice Doc Dept:
Invoice Doc ID:

Vendor Invoice Number:
Vendor Invoice Date:
Tracking Date:

2505

BainCor, Inc.

Invoice

763 South Street
Suite A
Holbrook, MA 02343

Phone: 339-987-5525
Fax: 339-987-5528
info@baincor.com

Date	Invoice #
3/16/2023	4146

Bill To

Massachusetts State Police
Division of Homeland Security and Prepare
Office of the Division Commander
Framingham, MA 01702

Ship To

P.O. Number	Terms	Rep	Ship	Via	F.O.B.	Project
PO-22-1084-POL...			3/16/2023			

Quantity	Item Code	Description	Price Each	Amount
12	misc	"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 Received on 4/6/2023 by: Sgt. N. Pack #3680	21,225.00	254,700.00

Invoice Receipt date 3/23/23
The equipment, goods or services for which this payment is made were received on 4/6/23
certified by
signature date

PVPOL7214230208AN

Unit# 7214
8000 4692

MassDOT State Wide Contract
INTF0000K03C00111753

Total

2506

BainCor, Inc.

Invoice

763 South Street
Suite A
Holbrook, MA 02343

Phone: 339-987-5525
Fax: 339-987-5528
info@baincor.com

Date	Invoice #
3/16/2023	4146

Bill To

Massachusetts State Police
Division of Homeland Security and Prepare
Office of the Division Commander
Framingham, MA 01702

Ship To

P.O. Number	Terms	Rep	Ship	Via	F.O.B.	Project
PO-22-1084-POL...			3/16/2023			

Quantity	Item Code	Description	Price Each	Amount
		VIN#"s 5F18S101XP1000800 5F18S1011P1000801 5F18S1013P1000802 5F18S1015P1000803 5F18S1017P1000804 5F18S1019P1000805 5F18S1010P1000806 5F18S1012P1000807 5F18S1014P1000808 5F18S1016P1000809 5F18S1012P1000810 5F18S1014P1000811 PO-22-1084-POLGH-GHQ-24335:2		
		Sales Tax	0.00%	0.00

MassDOT State Wide Contract
INTF0000K03C00111753

Total $254,700.00

⚠ Vendor Invoice added to Vendor Invoice Registry. (A1808)

Pymt Request-CommodityBased(PRC) **Dept:** POL **ID:** PVPOL7214125BAYSTA01 **Ver.:** 1 **Function:** New **Phase:** ~~Draft~~ Final Pg

Modified by polaj8 , 05/04/2023

Vendor **Total Lines:** 1 **Vendor Line:** 1 **Vendor Customer:** VC0000500765 **Legal Name:** BAY STATE ALARM SECURITY INC

	Vendor Line	Vendor Customer	Legal Name	Line Amount
	1	VC0000500765	BAY STATE ALARM SECURITY INC	151959.89

From 1 to 1 Total: 1 unit # 7214 FSHSP20CFC 8000-4692

General Information

Vendor Customer: VC0000500765
Legal Name: BAY STATE ALARM SECURI
Alias/DBA: BSA SECURITY INTEGRATC
Address Code: AD001
Address 1: 462 PLEASANT ST
Address 2:
City: MARLBOROUGH
State: Massachusetts
Zip Code: 01752-1127
Country: USA
County:

Vendor Contact ID:
Vendor Contact Name: Cindy McStay
Vendor Contact Phone: 508-485-1174
Vendor Contact Phone Ext.: 112
Vendor Contact Email: cindy@bsasi.com
Fax:
Fax Extension:
Web Address http://:
Taxpayer ID Number:
Taxpayer ID Type:
Merchant ID:
Tax Profile:
Received Service From Date:
Received Service To Date:

Disbursement Options

Disbursement Type: EFT
Disbursement Format: CTX
Scheduled Payment Date: 05/12/2023
Disbursement Priority: 99
Single Payment:
Pay Third Party:
On-line Disbursement Rqst:
EFT Status: Eligible for EFT

Handling Code:
Disbursement Category: 100

Invoice Information

Invoice Doc Code:
Invoice Doc Dept:
Invoice Doc ID:

Vendor Invoice Number:
Vendor Invoice Date:
Tracking Date:

BSASi Security Integrators

Bay State Alarm Security, Inc.
462 Pleasant Street, Marlboro, MA 01752
Phone 508-485-1174 Fax 508-624-6568

GSA Advantage!

INVOICE

Invoice Number: 11342
Invoice Date: Apr 3, 2023
Page: 1

04/04/2023

Bill To:

Massachusetts State Police General
470 Worcester Road
Framingham, MA 01702

Job:

2023BSASIU07POL20446
ALPR TRAILER
COMMONWEALTH FUSION CENTER

Customer ID	Customer PO	Payment Terms	
MA State Police	2023BSASIU07POL20446	Net 30 Days	
Service Tech ID	**Job Ticket ID**	**Date of Service**	**Due Date**
		4/4/23	5/3/23

Quantity	Item	Description	Unit Price	Amount
[redacted] G.L. c. 4.sec. 7. cl.26	Quoted Job -Material	Quoted Job -Material Includes [redacted] G.L. c. 4.sec. 7.cl.26 (n)(security) cameras and all related peripherals ALPR Neology Cameras Delivered 4/4/23	[redacted] G.L. c. 4.sec. 7. cl.26(f)(n)	151,959.89

P525
See Revised Invoice

Invoice date 4/5/23

Received date 5/3/2023

Approval Sgt. N. Pack #3680

Subtotal	151,959.89
Sales Tax	
Total Invoice Amount	151,959.89
Payment/Credit Applied	
TOTAL	**151,959.89**

Check/Credit Memo No:

PVPOL721423094/BaySta

FSHSP20CFC

unit #7214

800-4692

GSA Advantage!

SDVOSB

2509

BSASi Security Integrators

SDVOSB

Packing List

Bay State Alarm Security, Inc. * 462 Pleasant Street * Marlboro, MA 01752 Ph 508-485-1174 Fax 508-624-6568

To: **Massachusetts State Police**
21 Oak Street,
Leominster Ma 01453

Delivered 4/4/23

Facility: State Police
Contact: Sgt. Noah Pack

From:

Job: Provision of ALPR Trailer Components

Re: ALPR Trainer Components

#	QTY	U/M	DESCRIPTION		
1.	[redacted]	Ea	FC574250000 – NEOLOGY P525 CAMERA		
2.		Ea	HC350244L010 – NEOLOGY P525 POWER & SERIAL CABLE (10M)		
3.		Ea	HC350242L010 – SINGLE ETHERNET CABLE (10M)		
4.		Ea	HW25X0011 – NEOLOGY MOUNTING BRACKET		
5.		Ea	INJ-C201G-BT-24-T – ANTAIRA POE INJECTOR		
6.		Ea	TRACO TEP 100-1218 12VDC TO 48VDC POWER SUPPLY		
7.		Ea	MEAN WELL RS-1000-48 – 110VAC TO 48VDC POWER SUPPLY		
8.		Ea	FC4819730200 – NEOLOGY P497 CAMERAS		
9.		Ea	HC350228L005 – NEOLOGY GLANDED 5M CABLE FOR P497		
10.		Ea	P497MOUNT – MOUNTING BRACKET FOR P497 CAMERA		
11.		Ea	DDR-60G-15 – MEAN WELL 15VDC, 60W DC/DC CONVERTER		
12.		Ea	RHINO PSE15-160 – 110VAC TO 15VDC POWER SUPPLY		
13.		Ea	RV55 – SIERRA WIRELESS RV55 ROUTER		
14.		Ea	FXUB66.01.0150C – TAOGLAS MAXIMUS FLEXIBLE ANTENNA (SMA)		
15.		Ea	LNX-500A-T – ANTAIRA 12VDC, 10/100 SWITCH		
16.		Ea	BSA TOOL KIT – HAND TOOLS AND SOCKET SET KIT		

View All 1 of 5 | ⚠ Vendor Invoice added to Vendor Invoice Registry. (A1808)

Pymt Request-CommodityBased(PRC) **Dept:** POL **ID:** PVPOL721423INSIGH001 **Ver.:** 1 **Function:** New **Phase:** Draft Final POR

Modified by polajß , 04/03/2023

Vendor **Total Lines:** 1 **Vendor Line:** 1 **Vendor Customer:** VC6000239916 **Legal Name:** INSIGHT PUBLIC SECTOR INC

Vendor Line	Vendor Customer	Legal Name	Line Amount
1	VC6000239916	INSIGHT PUBLIC SECTOR INC	160442.91

From 1 to 1 Total: 1

8000-4692 FSHSP20CFC unit #7214

General Information

Vendor Customer: VC6000239916
Legal Name: INSIGHT PUBLIC SECTOR I
Alias/DBA:
Address Code: AD001
Address 1: PO BOX 731072
Address 2:
City: DALLAS
State: Texas
Zip Code: 75373-1072
Country: USA
County:

Vendor Contact ID:
Vendor Contact Name: DAVID RODRIGUEZ
Vendor Contact Phone: 800-467-4448
Vendor Contact Phone Ext.:
Vendor Contact Email: DRODRIGU@INSIGHT.COM
Fax:
Fax Extension:
Web Address http://:
Taxpayer ID Number:
Taxpayer ID Type:
Merchant ID:
Tax Profile:
Received Service From Date:
Received Service To Date:

Disbursement Options

Disbursement Type: EFT
Disbursement Format: CTX
Scheduled Payment Date: 05/04/2023
Disbursement Priority: 99
Single Payment:
Pay Third Party:
On-line Disbursement Rqst:
EFT Status: Eligible for EFT

Handling Code:
Disbursement Category: 100

Invoice Information

Invoice Doc Code:
Invoice Doc Dept:
Invoice Doc ID:

Vendor Invoice Number:
Vendor Invoice Date:
Tracking Date:

2511

Insight PUBLIC SECTOR

Ship To 10330021 Page 1 of 2
MASSACHUSETTS STATE POLICE
General Headquarters
Amy Thibault
470 WORCESTER RD
FRAMINGHAM MA 01702-5309

Invoice

Invoice No.	Date:	Sales Order No.	Account No.	Payment Terms	Due Date	Sales Rep Name	Account Clerk:
1101037368	23-MAR-2023	333319040	10330021	Net 45 Days	07-MAY-2023	Rosemarie Pavlick	Audi Chapin

PO No.	PO Release No:	Contract No.	State Contract No.	Ship Via
2023INSITU12POL20650				Electronic Delivery/ESD

		Service Order No	Service Rep Name	Original Invoice No
FEIN: 36-3949000				

Register for Electronic Invoicing at www.insight.com/einvoice

	Material	Material Description	Qty	Unit Price	Extended Price
*	D0PR8LL-HAR	i2 Analysts Notebook Premium - trade-up license + 1 Year Software Subscription and Support - 1 concurrent user - Coverage Dates: 03-FEB-2023 - 03-FEB-2024 License Type: License with Maintenance and Support Media Type: ESD COMMONWEALTH OF MASSACHUSETTS SOFTWARE AND SERVICES(# ITS75)	9	12,833.44	115,500.96
*	E0DQWLL-HAR	i2 Analysts Notebook Premium - Software Subscription and Support Renewal (1 year) - 1 concurrent user - Coverage Dates: 22-MAR-2023 - 22-MAR-2024 License Type: License with Maintenance and Support Media Type: ESD COMMONWEALTH OF MASSACHUSETTS SOFTWARE AND SERVICES(# ITS75)	9	4,993.55	44,941.95

Sub Total	160,442.91
Ttl Freight Charge	0.00
Total Amount Due	160,442.91
Currency	USD

(T) Denotes taxable item * Denotes non-shippable item

Insight PUBLIC SECTOR

Please Remit To:
Insight Public Sector, Inc.
P.O. Box 731072
DALLAS TX 75373-1072

Send address changes to addresschange@insight.com

For proper credit, please return this portion with payment.

Ship To 10330021
MASSACHUSETTS STATE POLICE
General Headquarters
Amy Thibault
470 WORCESTER RD
FRAMINGHAM MA 01702-5309

ACCOUNT NO	10330021
INVOICE DATE	23-MAR-2023
INVOICE NUMBER	1101037368
BALANCE DUE	160,442.91
Amount Paid	
CURRENCY	USD

Bill to: 10330021
MASSACHUSETTS STATE POLICE
Kellie Gray - kellie.gray@pol.state.ma.u
470 WORCESTER RD
FRAMINGHAM MA 01702-5309

Please remit electronically to:
Insight Public Sector, Inc
c/o JPMorgan Chase
Account: [redacted]
Swift code: chasus33
Wire ABA: [redacted]
ACH ABA:

8000-4692
PVPOL 721423 INSIGHT001

00103300210110103736800016044291349700000000000000

Unit #7214 FSHSP20CFC

2512

Invoice Date 03/27/2023
Received Date
Approval

Insight.
PUBLIC SECTOR

Ship To 10330021
MASSACHUSETTS STATE POLICE
General Headquarters
Amy Thibault
470 WORCESTER RD
FRAMINGHAM MA 01702-5309

Invoice

Invoice No.	Date:	Sales Order No.	Account No.	Payment Terms	Due Date	Sales Rep Name	Account Clerk:
1101037368	23-MAR-2023	333319040	10330021	Net 45 Days	07-MAY-2023	Rosemarie Pavlick	Audi Chapin

PO No.	PO Release No:	Contract No.	State Contract No.	Ship Via
2023INSITU12POL20650				Electronic Delivery/ESD

		Service Order No	Service Rep Name	Original Invoice No
FEIN: 36-3949000				

Register for Electronic Invoicing at www.insight.com/einvoice

Material	Material Description	Qty	Unit Price	Extended Price

THANK YOU FOR YOUR ORDER.
FOR ALL INQUIRIES PLEASE CALL 800-934-4477.
The Terms and Conditions and Return Policy and Procedures set forth on www.ips.insight.com/TermsandConditions are specifically incorporated herein unless purchase is being made pursuant to a separate written agreement in which case the terms of the separate written agreement shall govern.

Invoice Receipt date 3/28/23

"The equipment, goods or services for which this payment is made were received on 3/23/23

certified by Amy Thibault

signature date 3/30/23

Grant Program Spending Report

Appropriation	Program	BFY	Doc_ID_Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
Dept: POL										
80004692	HOMELAND SECURITY II									
FSHSP20CFC	COMMONWEALTH FUSION CENTER									
		2022								
object_class	AA									
A01	Salaries: Inclusive									
			PREXPPOL	EMPL 020210731148138		$2,025.00		8/3/2021	8/3/2021	8/3/2021
			PRLNPPOL	EMPL 020210731148138		$2,025.00		8/3/2021	8/3/2021	8/3/2021
			PRLNPPOL	EMPL 020210731148138		($2,025.00)		8/3/2021	8/3/2021	8/3/2021
			PREXPPOL	EMPL 020210814141338		$1,830.00		8/17/2021	8/17/2021	8/17/2021
			PRLNPPOL	EMPL 020210814141338		$1,830.00		8/17/2021	8/17/2021	8/17/2021
			PRLNPPOL	EMPL 020210814141338		($1,830.00)		8/17/2021	8/17/2021	8/17/2021
			PREXPPOL	EMPL 020210828150808		$2,610.00		8/31/2021	8/31/2021	8/31/2021
			PRLNPPOL	EMPL 020210828150808		$2,610.00		8/31/2021	8/31/2021	8/31/2021
			PRLNPPOL	EMPL 020210828150808		($2,610.00)		8/31/2021	8/31/2021	8/31/2021
			PREXPPOL	EMPL 020210911142238		$1,680.00		9/14/2021	9/14/2021	9/14/2021
			PRLNPPOL	EMPL 020210911142238		($1,680.00)		9/14/2021	9/14/2021	9/14/2021
			PRLNPPOL	EMPL 020210911142238		$1,680.00		9/14/2021	9/14/2021	9/14/2021
			PREXPPOL	EMPL 020210925147338		$1,950.00		9/28/2021	9/28/2021	9/28/2021
			PRLNPPOL	EMPL 020210925147338		($1,950.00)		9/28/2021	9/28/2021	9/28/2021
			PRLNPPOL	EMPL 020210925147338		$1,950.00		9/28/2021	9/28/2021	9/28/2021
			PREXPPOL	EMPL 020211009159078		$2,520.00		10/12/2021	10/12/2021	10/12/2021
			PRLNPPOL	EMPL 020211009159078		$2,520.00		10/12/2021	10/12/2021	10/12/2021
			PRLNPPOL	EMPL 020211009159078		($2,520.00)		10/12/2021	10/12/2021	10/12/2021
			PREXPPOL	EMPL 020211023149008		$2,850.00		10/26/2021	10/26/2021	10/26/2021
			PRLNPPOL	EMPL 020211023149008		($2,850.00)		10/26/2021	10/26/2021	10/26/2021
			PRLNPPOL	EMPL 020211023149008		$2,850.00		10/26/2021	10/26/2021	10/26/2021
			PREXPPOL	EMPL 020211106154318		$2,670.00		11/9/2021	11/9/2021	11/9/2021
			PRLNPPOL	EMPL 020211106154318		$2,670.00		11/9/2021	11/9/2021	11/9/2021
			PRLNPPOL	EMPL 020211106154318		($2,670.00)		11/9/2021	11/9/2021	11/9/2021
			PREXPPOL	EMPL 020211120148528		$2,685.00		11/23/2021	11/23/2021	11/23/2021
			PRLNPPOL	EMPL 020211120148528		($2,685.00)		11/23/2021	11/23/2021	11/23/2021
			PRLNPPOL	EMPL 020211120148528		$2,685.00		11/23/2021	11/23/2021	11/23/2021
			PREXPPOL	EMPL 020211204154398		$2,040.00		12/7/2021	12/7/2021	12/7/2021
			PRLNPPOL	EMPL 020211204154398		$2,040.00		12/7/2021	12/7/2021	12/7/2021
			PRLNPPOL	EMPL 020211204154398		($2,040.00)		12/7/2021	12/7/2021	12/7/2021
			PREXPPOL	EMPL 020211218141808		$1,935.00		12/21/2021	12/21/2021	12/21/2021
			PRLNPPOL	EMPL 020211218141808		($1,935.00)		12/21/2021	12/21/2021	12/21/2021
			PRLNPPOL	EMPL 020211218141808		$1,935.00		12/21/2021	12/21/2021	12/21/2021
			PREXPPOL	EMPL 020220101155948		$1,035.00		1/4/2022	1/4/2022	1/4/2022
			PRLNPPOL	EMPL 020220101155948		$1,035.00		1/4/2022	1/4/2022	1/4/2022
			PRLNPPOL	EMPL 020220101155948		($1,035.00)		1/4/2022	1/4/2022	1/4/2022
			PREXPPOL	EMPL 020220115135688		$2,055.00		1/18/2022	1/18/2022	1/18/2022
			PRLNPPOL	EMPL 020220115135688		$2,055.00		1/18/2022	1/18/2022	1/18/2022
			PRLNPPOL	EMPL 020220115135688		($2,055.00)		1/18/2022	1/18/2022	1/18/2022
			PREXPPOL	EMPL 020220129149508		$2,595.00		2/1/2022	2/1/2022	2/1/2022
			PRLNPPOL	EMPL 020220129149508		$2,595.00		2/1/2022	2/1/2022	2/1/2022
			PRLNPPOL	EMPL 020220129149508		($2,595.00)		2/1/2022	2/1/2022	2/1/2022
			PREXPPOL	EMPL 020220212156038		$1,920.00		2/15/2022	2/15/2022	2/15/2022
			PRLNPPOL	EMPL 020220212156038		$1,920.00		2/15/2022	2/15/2022	2/15/2022
			PRLNPPOL	EMPL 020220212156038		($1,920.00)		2/15/2022	2/15/2022	2/15/2022
			PREXPPOL	EMPL 020220226134278		$1,260.00		3/1/2022	3/1/2022	3/1/2022
			PRLNPPOL	EMPL 020220226134278		($1,260.00)		3/1/2022	3/1/2022	3/1/2022
			PRLNPPOL	EMPL 020220226134278		$1,260.00		3/1/2022	3/1/2022	3/1/2022
			PREXPPOL	EMPL 020220312135738		$2,250.00		3/15/2022	3/15/2022	3/15/2022

Appropriation	Program	BFY	Doc_ID	Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
PRLNP	POL		EMPL 020220312135738				($2,250.00)			3/15/2022 3/15/2022	3/15/2022
PRLNP	POL		EMPL 020220312135738				$2,250.00			3/15/2022 3/15/2022	3/15/2022
PREXP	POL		EMPL 020220326137338				$3,000.00			3/29/2022 3/29/2022	3/29/2022
PRLNP	POL		EMPL 020220326137338				$3,000.00			3/29/2022 3/29/2022	3/29/2022
PRLNP	POL		EMPL 020220326137338				($3,000.00)			3/29/2022 3/29/2022	3/29/2022
PREXP	POL		EMPL 020220409137648				$2,820.00			4/12/2022 4/12/2022	4/12/2022
PRLNP	POL		EMPL 020220409137648				($2,820.00)			4/12/2022 4/12/2022	4/12/2022
PRLNP	POL		EMPL 020220409137648				$2,820.00			4/12/2022 4/12/2022	4/12/2022
PREXP	POL		EMPL 020220423149038				$2,325.00			4/26/2022 4/26/2022	4/26/2022
PRLNP	POL		EMPL 020220423149038				$2,325.00			4/26/2022 4/26/2022	4/26/2022
PRLNP	POL		EMPL 020220423149038				($2,325.00)			4/26/2022 4/26/2022	4/26/2022
PREXP	POL		EMPL 020220507136008				$1,905.00			5/10/2022 5/10/2022	5/10/2022
PRLNP	POL		EMPL 020220507136008				$1,905.00			5/10/2022 5/10/2022	5/10/2022
PRLNP	POL		EMPL 020220507136008				($1,905.00)			5/10/2022 5/10/2022	5/10/2022
PREXP	POL		EMPL 020220521150458				$2,130.00			5/24/2022 5/24/2022	5/24/2022
PRLNP	POL		EMPL 020220521150458				($2,130.00)			5/24/2022 5/24/2022	5/24/2022
PRLNP	POL		EMPL 020220521150458				$2,130.00			5/24/2022 5/24/2022	5/24/2022
PREXP	POL		EMPL 020220604123828				$480.00			6/7/2022 6/7/2022	6/7/2022
PRLNP	POL		EMPL 020220604123828				($480.00)			6/7/2022 6/7/2022	6/7/2022
PRLNP	POL		EMPL 020220604123828				$480.00			6/7/2022 6/7/2022	6/7/2022
Summary for 'Object' = A01 (69 detail records)							*$48,570.00*				
Summary for 'Object_Class' = AA (69 detail records)							*$48,570.00*				

object_class BB

B01 Other Out Of State Travel - INCLUSIVE: AIRFARE, HOTEL, LODGI

PREXP	POL		EMPL 020211009159058				$1,974.46			10/12/2021 10/12/2021	10/12/2021
PRLNP	POL		EMPL 020211009159058				($1,974.46)			10/12/2021 10/12/2021	10/12/2021
PRLNP	POL		EMPL 020211009159058				$1,974.46			10/12/2021 10/12/2021	10/12/2021
PREXP	POL		EMPL 020211204154378				$689.40			12/7/2021 12/7/2021	12/7/2021
PRLNP	POL		EMPL 020211204154378				($689.40)			12/7/2021 12/7/2021	12/7/2021
PRLNP	POL		EMPL 020211204154378				$689.40			12/7/2021 12/7/2021	12/7/2021
PREXP	POL		EMPL 020220226134268				$1,598.08			3/1/2022 3/1/2022	3/1/2022
PRLNP	POL		EMPL 020220226134268				$1,598.08			3/1/2022 3/1/2022	3/1/2022
PRLNP	POL		EMPL 020220226134268				($1,598.08)			3/1/2022 3/1/2022	3/1/2022
Summary for 'Object' = B01 (9 detail records)							*$4,261.94*				

B02 In-State Travel

PREXP	POL		EMPL 020220226134268				$175.21			3/1/2022 3/1/2022	3/1/2022
PRLNP	POL		EMPL 020220226134268				($175.21)			3/1/2022 3/1/2022	3/1/2022
PRLNP	POL		EMPL 020220226134268				$175.21			3/1/2022 3/1/2022	3/1/2022
PREXP	POL		EMPL 020220702103958				$55.57			7/6/2022 7/6/2022	7/6/2022
PRLNP	POL		EMPL 020220702103958				$55.57			7/6/2022 7/6/2022	7/6/2022
PRLNP	POL		EMPL 020220702103958				($55.57)			7/6/2022 7/6/2022	7/6/2022
Summary for 'Object' = B02 (6 detail records)							*$230.78*				

B05 Conference, Training, Registration and Membership Dues and L

PREXP	POL		EMPL 020211009159058				$550.00			10/12/2021 10/12/2021	10/12/2021
PRLNP	POL		EMPL 020211009159058				$550.00			10/12/2021 10/12/2021	10/12/2021
PRLNP	POL		EMPL 020211009159058				($550.00)			10/12/2021 10/12/2021	10/12/2021
PREXP	POL		EMPL 020211204154378				$150.00			12/7/2021 12/7/2021	12/7/2021
PRLNP	POL		EMPL 020211204154378				$150.00			12/7/2021 12/7/2021	12/7/2021
PRLNP	POL		EMPL 020211204154378				($150.00)			12/7/2021 12/7/2021	12/7/2021
PREXP	POL		EMPL 020220226134268				$550.00			3/1/2022 3/1/2022	3/1/2022
PRLNP	POL		EMPL 020220226134268				($550.00)			3/1/2022 3/1/2022	3/1/2022
PRLNP	POL		EMPL 020220226134268				$550.00			3/1/2022 3/1/2022	3/1/2022
PREXP	POL		EMPL 020220326137328				$154.00			3/29/2022 3/29/2022	3/29/2022
PRLNP	POL		EMPL 020220326137328				($154.00)			3/29/2022 3/29/2022	3/29/2022
PRLNP	POL		EMPL 020220326137328				$154.00			3/29/2022 3/29/2022	3/29/2022
Summary for 'Object' = B05 (12 detail records)							*$1,404.00*				
Summary for 'Object_Class' = BB (27 detail records)							*$5,896.72*				

Appropriation	Program	BFY	Doc_ID_Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
2515										
object_class	CC									
C23	Management, Business Professionals & Admin Services									
PREXPPOL				CNTR 020210731105478		$3,000.00			8/3/2021	8/3/2021	8/3/2021
PRLNPPOL				CNTR 020210731105478		($3,000.00)			8/3/2021	8/3/2021	8/3/2021
PRLNPPOL				CNTR 020210731105478		$3,000.00			8/3/2021	8/3/2021	8/3/2021
PREXPPOL				CNTR 020210814103948		$3,000.00			8/17/2021	8/17/2021	8/17/2021
PRLNPPOL				CNTR 020210814103948		$3,000.00			8/17/2021	8/17/2021	8/17/2021
PRLNPPOL				CNTR 020210814103948		($3,000.00)			8/17/2021	8/17/2021	8/17/2021
PREXPPOL				CNTR 020210828104868		$3,000.00			8/31/2021	8/31/2021	8/31/2021
PRLNPPOL				CNTR 020210828104868		$3,000.00			8/31/2021	8/31/2021	8/31/2021
PRLNPPOL				CNTR 020210828104868		($3,000.00)			8/31/2021	8/31/2021	8/31/2021
PREXPPOL				CNTR 020210911103958		$3,000.00			9/14/2021	9/14/2021	9/14/2021
PRLNPPOL				CNTR 020210911103958		($3,000.00)			9/14/2021	9/14/2021	9/14/2021
PRLNPPOL				CNTR 020210911103958		$3,000.00			9/14/2021	9/14/2021	9/14/2021
PRADJPOL				09152100000000004355		$580.00			9/15/2021	9/15/2021	9/15/2021
PRADJPOL				09152100000000004356		$3,035.00			9/15/2021	9/15/2021	9/15/2021
PREXPPOL				CNTR 020210925104818		$3,000.00			9/28/2021	9/28/2021	9/28/2021
PRLNPPOL				CNTR 020210925104818		($3,000.00)			9/28/2021	9/28/2021	9/28/2021
PRLNPPOL				CNTR 020210925104818		$3,000.00			9/28/2021	9/28/2021	9/28/2021
PREXPPOL				CNTR 020211009107198		$3,000.00			10/12/2021	10/12/2021	10/12/2021
PRLNPPOL				CNTR 020211009107198		$3,000.00			10/12/2021	10/12/2021	10/12/2021
PRLNPPOL				CNTR 020211009107198		($3,000.00)			10/12/2021	10/12/2021	10/12/2021
PREXPPOL				CNTR 020211023106928		$3,000.00			10/26/2021	10/26/2021	10/26/2021
PRLNPPOL				CNTR 020211023106928		$3,000.00			10/26/2021	10/26/2021	10/26/2021
PRLNPPOL				CNTR 020211023106928		($3,000.00)			10/26/2021	10/26/2021	10/26/2021
PREXPPOL				CNTR 020211106106858		$3,000.00			11/9/2021	11/9/2021	11/9/2021
PRLNPPOL				CNTR 020211106106858		($3,000.00)			11/9/2021	11/9/2021	11/9/2021
PRLNPPOL				CNTR 020211106106858		$3,000.00			11/9/2021	11/9/2021	11/9/2021
PREXPPOL				CNTR 020211120106908		$3,000.00			11/23/2021	11/23/2021	11/23/2021
PRLNPPOL				CNTR 020211120106908		($3,000.00)			11/23/2021	11/23/2021	11/23/2021
PRLNPPOL				CNTR 020211120106908		$3,000.00			11/23/2021	11/23/2021	11/23/2021
PREXPPOL				CNTR 020211204107268		$3,000.00			12/7/2021	12/7/2021	12/7/2021
PRLNPPOL				CNTR 020211204107268		($3,000.00)			12/7/2021	12/7/2021	12/7/2021
PRLNPPOL				CNTR 020211204107268		$3,000.00			12/7/2021	12/7/2021	12/7/2021
PREXPPOL				CNTR 020211218104668		$3,000.00			12/21/2021	12/21/2021	12/21/2021
PRLNPPOL				CNTR 020211218104668		($3,000.00)			12/21/2021	12/21/2021	12/21/2021
PRLNPPOL				CNTR 020211218104668		$3,000.00			12/21/2021	12/21/2021	12/21/2021
PREXPPOL				CNTR 020220101104698		$3,000.00			1/4/2022	1/4/2022	1/4/2022
PRLNPPOL				CNTR 020220101104698		($3,000.00)			1/4/2022	1/4/2022	1/4/2022
PRLNPPOL				CNTR 020220101104698		$3,000.00			1/4/2022	1/4/2022	1/4/2022
PREXPPOL				CNTR 020220115102868		$3,000.00			1/18/2022	1/18/2022	1/18/2022
PRLNPPOL				CNTR 020220115102868		$3,000.00			1/18/2022	1/18/2022	1/18/2022
PRLNPPOL				CNTR 020220115102868		($3,000.00)			1/18/2022	1/18/2022	1/18/2022
PREXPPOL				CNTR 020220129106238		$3,000.00			2/1/2022	2/1/2022	2/1/2022
PRLNPPOL				CNTR 020220129106238		($3,000.00)			2/1/2022	2/1/2022	2/1/2022
PRLNPPOL				CNTR 020220129106238		$3,000.00			2/1/2022	2/1/2022	2/1/2022
PREXPPOL				CNTR 020220212107738		$3,000.00			2/15/2022	2/15/2022	2/15/2022
PRLNPPOL				CNTR 020220212107738		$3,000.00			2/15/2022	2/15/2022	2/15/2022
PRLNPPOL				CNTR 020220212107738		($3,000.00)			2/15/2022	2/15/2022	2/15/2022
PREXPPOL				CNTR 020220226102998		$3,000.00			3/1/2022	3/1/2022	3/1/2022
PRLNPPOL				CNTR 020220226102998		($3,000.00)			3/1/2022	3/1/2022	3/1/2022
PRLNPPOL				CNTR 020220226102998		$3,000.00			3/1/2022	3/1/2022	3/1/2022
PREXPPOL				CNTR 020220312103008		$3,000.00			3/15/2022	3/15/2022	3/15/2022
PRLNPPOL				CNTR 020220312103008		($3,000.00)			3/15/2022	3/15/2022	3/15/2022
PRLNPPOL				CNTR 020220312103008		$3,000.00			3/15/2022	3/15/2022	3/15/2022
PREXPPOL				CNTR 020220326103218		$3,000.00			3/29/2022	3/29/2022	3/29/2022
PRLNPPOL				CNTR 020220326103218		$3,000.00			3/29/2022	3/29/2022	3/29/2022
PRLNPPOL				CNTR 020220326103218		($3,000.00)			3/29/2022	3/29/2022	3/29/2022
PREXPPOL				CNTR 020220409103208		$3,000.00			4/12/2022	4/12/2022	4/12/2022

Appropriation	Program	BFY	Doc_ID_Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
PRLNP	POL		CNTR 020220409103208			$3,000.00			4/12/2022 4/12/2022	4/12/2022
PRLNP	POL		CNTR 020220409103208			($3,000.00)			4/12/2022 4/12/2022	4/12/2022
PREXP	POL		CNTR 020220423106868			$3,000.00			4/26/2022 4/26/2022	4/26/2022
PRLNP	POL		CNTR 020220423106868			($3,000.00)			4/26/2022 4/26/2022	4/26/2022
PRLNP	POL		CNTR 020220423106868			$3,000.00			4/26/2022 4/26/2022	4/26/2022
PREXP	POL		CNTR 020220507102968			$3,000.00			5/10/2022 5/10/2022	5/10/2022
PRLNP	POL		CNTR 020220507102968			($3,000.00)			5/10/2022 5/10/2022	5/10/2022
PRLNP	POL		CNTR 020220507102968			$3,000.00			5/10/2022 5/10/2022	5/10/2022
PREXP	POL		CNTR 020220521106788			$3,000.00			5/24/2022 5/24/2022	5/24/2022
PRLNP	POL		CNTR 020220521106788			$3,000.00			5/24/2022 5/24/2022	5/24/2022
PRLNP	POL		CNTR 020220521106788			($3,000.00)			5/24/2022 5/24/2022	5/24/2022
PREXP	POL		CNTR 020220604105068			$3,000.00			6/7/2022 6/7/2022	6/7/2022
PRLNP	POL		CNTR 020220604105068			$3,000.00			6/7/2022 6/7/2022	6/7/2022
PRLNP	POL		CNTR 020220604105068			($3,000.00)			6/7/2022 6/7/2022	6/7/2022
PREXP	POL		CNTR 020220618107118			$3,000.00			6/21/2022 6/21/2022	6/21/2022
PRLNP	POL		CNTR 020220618107118			($3,000.00)			6/21/2022 6/21/2022	6/21/2022
PRLNP	POL		CNTR 020220618107118			$3,000.00			6/21/2022 6/21/2022	6/21/2022
Summary for 'Object' = C23 (74 detail records)						*$75,615.00*				
C98 Reimb Travel/Other Expenses CC Special Contract/Employee										
PREXP	POL		CNTR 020211218104658			$7.59			12/21/2021 12/21/2021	12/21/2021
PREXP	POL		CNTR 020211218104668			$26.16			12/21/2021 12/21/2021	12/21/2021
PRLNP	POL		CNTR 020211218104658			($7.59)			12/21/2021 12/21/2021	12/21/2021
PRLNP	POL		CNTR 020211218104668			$26.16			12/21/2021 12/21/2021	12/21/2021
PRLNP	POL		CNTR 020211218104668			($26.16)			12/21/2021 12/21/2021	12/21/2021
PRLNP	POL		CNTR 020211218104658			$7.59			12/21/2021 12/21/2021	12/21/2021
Summary for 'Object' = C98 (6 detail records)						*$33.75*				
Summary for 'Object_Class' = CC (80 detail records)						*$75,648.75*				
object_class DD										
D09 Fringe Benefit Cost Recoupment										
CA	CTR		FRGEFRNG0911210000001792			$2,421.79				9/11/2021
CA	CTR		PTXEPYTX0911210000007408			$127.36				9/11/2021
CA	CTR		PTXEPYTX0911210000007689			$177.30				9/11/2021
CA	CTR		FRGEFRNG1010210000002420			$1,359.80				10/10/2021
CA	CTR		PTXEPYTX1010210000010429			$189.42				10/10/2021
CA	CTR		PTXEPYTX1010210000010036			$71.51				10/10/2021
CA	CTR		FRGEFRNG1107210000003062			$2,011.60				11/7/2021
CA	CTR		PTXEPYTX1107210000012600			$105.79				11/7/2021
CA	CTR		PTXEPYTX1107210000012898			$118.20				11/7/2021
CA	CTR		FRGEFRNG1204210000003705			$2,005.98				12/4/2021
CA	CTR		PTXEPYTX1204210000015329			$118.20				12/4/2021
CA	CTR		PTXEPYTX1204210000015063			$105.49				12/4/2021
CA	CTR		FRGEFRNG0115220000004349			$1,489.04				1/15/2022
CA	CTR		PTXEPYTX0115220000018441			$118.20				1/15/2022
CA	CTR		PTXEPYTX0115220000018007			$78.31				1/15/2022
CA	CTR		FRGEFRNG0205220000004987			$1,157.51				2/5/2022
CA	CTR		PTXEPYTX0205220000021134			$118.20				2/5/2022
CA	CTR		PTXEPYTX0205220000020855			$60.87				2/5/2022
CA	CTR		FRGEFRNG0305220000005627			$1,691.32				3/5/2022
CA	CTR		PTXEPYTX0305220000023716			$118.20				3/5/2022
CA	CTR		PTXEPYTX0305220000023426			$88.95				3/5/2022
CA	CTR		FRGEFRNG0409220000006301			$2,438.65				4/9/2022
CA	CTR		PTXEPYTX0409220000026119			$128.25				4/9/2022
CA	CTR		PTXEPYTX0409220000026405			$177.30				4/9/2022
CA	CTR		FRGEFRNG0507220000006969			$1,927.32				5/7/2022
CA	CTR		PTXEPYTX0507220000028701			$101.36				5/7/2022
CA	CTR		PTXEPYTX0507220000028979			$118.20				5/7/2022
CA	CTR		FRGEFRNG0611220000007635			$1,511.51				6/11/2022
CA	CTR		PTXEPYTX0611220000031524			$118.20				6/11/2022

Appropriation	Program	BFY	Doc_ID_Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
CA CTR	PTXEPYTX0611220000031281					$79.49				6/11/2022
CA CTR	FRGEFRNG0709220000000330					$179.81				7/9/2022
CA CTR	PTXEPYTX0709220000002583					$118.20				7/9/2022
CA CTR	PTXEPYTX0709220000002214					$9.46				7/9/2022
Summary for 'Object' = D09 (33 detail records)						*$20,640.79*				
Summary for 'Object_Class' = DD (33 detail records)						*$20,640.79*				

object_class EE

E16 Indirect Cost Recoupment

CA CTR	INDE INDC0911210000002832					$1,134.61				9/11/2021
CA CTR	INDE INDC1010210000003717					$637.07				10/10/2021
CA CTR	INDE INDC1107210000004605					$942.44				11/7/2021
CA CTR	INDE INDC1204210000005527					$939.80				12/4/2021
CA CTR	INDE INDC0115220000006558					$697.61				1/15/2022
CA CTR	INDE INDC0205220000007471					$542.30				2/5/2022
CA CTR	INDE INDC0305220000008434					$792.38				3/5/2022
CA CTR	INDE INDC0409220000009381					$1,142.51				4/9/2022
CA CTR	INDE INDC0507220000010368					$902.95				5/7/2022
CA CTR	INDE INDC0611220000011310					$708.14				6/11/2022
CA CTR	INDE INDC0709220000000980					$84.24				7/9/2022
Summary for 'Object' = E16 (11 detail records)						*$8,524.05*				
Summary for 'Object_Class' = EE (11 detail records)						*$8,524.05*				

object_class UU

U03 Software & Information Technology Licenses (IT)

PRC	POL 7214	PVPOL721422146SHI732	VC6000227588	SHI INTERNATIONAL CORP	B15154290	5/2/2022	$22,880.00	$0.00	$22,880.00	5/9/2022	5/9/2022	5/27/2022
EFT	CTR	DISB0613220000127079	VC6000227588	SHI INTERNATIONAL CORP	B15154290	5/2/2022	($22,880.00)			5/9/2022	5/9/2022	6/13/2022
EFT	CTR	DISB0613220000127079	VC6000227588	SHI INTERNATIONAL CORP	B15154290	5/2/2022	$22,880.00			5/9/2022	5/9/2022	6/13/2022
Summary for 'Object' = U03 (3 detail records)							*$22,880.00*	*$0.00*	*$22,880.00*			

U10 Information Tech (IT) Equipment Maintenance & Repair

EFT	CTR	DISB0311220000326501	VC6000227588	SHI INTERNATIONAL CORP	B13716166	1/20/2022	$136.00			1/13/2022	6/30/2022	3/11/2022
EFT	CTR	DISB0311220000326501	VC6000227588	SHI INTERNATIONAL CORP	B13716166	1/20/2022	($136.00)			1/13/2022	6/30/2022	3/11/2022
PRC	POL 7214	PVPOL721422068SHI129	VC6000227588	SHI INTERNATIONAL CORP	B13716166	1/20/2022	$136.00	$0.00	$136.00	1/13/2022	6/30/2022	3/11/2022
Summary for 'Object' = U10 (3 detail records)							*$136.00*	*$0.00*	*$136.00*			
Summary for 'Object_Class' = UU (6 detail records)							*$23,016.00*	*$0.00*	*$23,016.00*			
Summary for 'budget_fiscal_year' = 2022 (226 detail records)							*$182,296.31*	*$0.00*	*$23,016.00*			

2023

object_class KK

K10 Law Enforcement & Security Equipment

PRC	POL 7214	PVPOL721423102BAIN01	VC0000506451	BAIN COR INC	4146	3/23/2023	$254,700.00	$5,094.00	$249,606.00	4/6/2023	4/6/2023	4/13/2023
EFT	CTR	DISB0414230000460744	VC0000506451	BAIN COR INC	4146	3/23/2023	($5,094.00)			4/6/2023	4/6/2023	4/14/2023
EFT	CTR	DISB0414230000460744	VC0000506451	BAIN COR INC	4146	3/23/2023	$254,700.00			4/6/2023	4/6/2023	4/14/2023
EFT	CTR	DISB0414230000460744	VC0000506451	BAIN COR INC	4146	3/23/2023	($254,700.00)			4/6/2023	4/6/2023	4/14/2023
Summary for 'Object' = K10 (4 detail records)							*$249,606.00*	*$5,094.00*	*$249,606.00*			
Summary for 'Object_Class' = KK (4 detail records)							*$249,606.00*	*$5,094.00*	*$249,606.00*			

object_class UU

U07 Information Technology (IT) Equipment

PRC	POL 7214	PVPOL7214125BAYSTA01	VC0000500765	BAY STATE ALARM SECURITY INC	11342	4/5/2023	$151,959.89	$3,039.20	$148,920.69	5/3/2023	5/3/2023	5/8/2023
EFT	CTR	DISB0512230000053481	VC0000500765	BAY STATE ALARM SECURITY INC	11342	4/5/2023	$151,959.89			5/3/2023	5/3/2023	5/12/2023
EFT	CTR	DISB0512230000053481	VC0000500765	BAY STATE ALARM SECURITY INC	11342	4/5/2023	($151,959.89)			5/3/2023	5/3/2023	5/12/2023
EFT	CTR	DISB0512230000053481	VC0000500765	BAY STATE ALARM SECURITY INC	11342	4/5/2023	($3,039.20)			5/3/2023	5/3/2023	5/12/2023
Summary for 'Object' = U07 (4 detail records)							*$148,920.69*	*$3,039.20*	*$148,920.69*			

U12 Information Tech (IT) cloud services

PRC	POL 7214	PVPOL721423INSIGH001	VC6000239916	INSIGHT PUBLIC SECTOR INC	1101037368	3/23/2023	$160,442.91	$0.00	$160,442.91	3/23/2023	3/23/2023	4/10/2023
EFT	CTR	DISB0504230000030197	VC6000239916	INSIGHT PUBLIC SECTOR INC	1101037368	3/23/2023	$160,442.91			3/23/2023	3/23/2023	5/4/2023

Appropriation	Program	BFY	Doc_ID_Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
2516										
EFT CTR	DISB0504230000030197	VC6000239916	INSIGHT PUBLIC SECTOR INC	1101037368	3/23/2023	($160,442.91)			3/23/2023 3/23/2023	5/4/2023
Summary for 'Object' = U12 (3 detail records)						*$160,442.91*	*$0.00*	*$160,442.91*		
Summary for 'Object_Class' = UU (7 detail records)						*$309,363.60*	*$3,039.20*	*$309,363.60*		
Summary for 'budget_fiscal_year' = 2023 (11 detail records)						*$558,969.60*	*$8,133.20*	*$558,969.60*		
Summary for 'Program' = FSHSP20CFC (237 detail records)						*$741,265.91*	*$8,133.20*	*$581,985.60*		
Summary for 'Appropriation' = 80004692 (237 detail records)						*$741,265.91*	*$8,133.20*	*$581,985.60*		
Summary for 'Department' = POL (237 detail records)						*$741,265.91*	*$8,133.20*	*$581,985.60*		

Appropriation_Program	BFY	Doc_ID_Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
2519									
Grand Total					*$741,265.91*	*$8,133.20*	*$581,985.60*		

Form Name: 2520
Submission Time:
Browser:
IP Address:
Unique ID:
Location:

HLS Quarterly Report
July 13, 2023 1:24 pm
Chrome 114.0.0.0 / Windows
170.63.192.1
1120898790

Which subrecipient are you reporting data for in this quarterly progress report?	Other Agency
Please select which other agency you are reporting data for in this quarterly report.	MSP Commonwealth Fusion Center (CFC)

Reporting Information

Project Name	FSHSP20CFC
Federal Fiscal Year (FFY) Funding	FFY 2020

Contact Information

Reported by	Amy Thibault
Job Title	Intelligence Services Manager
Email Address	amy.thibault@pol.state.ma.us
Phone Number	(978) 451-3717

Reporting Period

Quarter Number	2
Reporting Period (Months)	April 1st - June 30th
Reporting Period (Year)	2023

Instructions

I. Planning

II. Organization

Regional Specialty Response Teams

III. Equipment

Equipment State Share Text	LPR trailers and cameras were received, and old equipment is being replaced or repaired. Approximately $5700 of additional equipment was quoted and ordered during Q2. It is anticipated that supplies will be ordered with the remaining funds as approved in the grant modification from November 2022.

IV. Training

Exercise Program

Type of exercise	Seminar

V. Management and Administration

VI. Other Activities

VII. Challenges/Delays

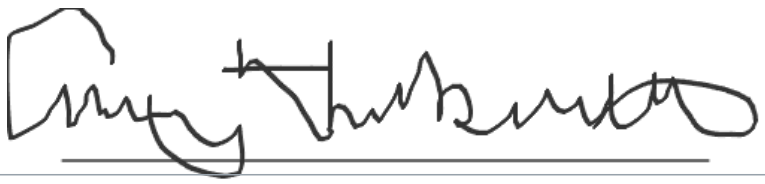
VIII. Success Stories

IX. Meetings

Waste, Fraud, or Abuse

Are you aware of any concerns regarding waste, fraud, or abuse connected to any of the grant-funded activities described in this report?	No

Fiduciary Coordinator Signature

Electronic Signature	
Date	Jul 13, 2023

Submitting Your QR

2523

Massachusetts Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Grant Division

QUARTERLY FINANCIAL REPORT

Agency/Contractor Name:	Massachusetts State Police	**Date:**	Thursday, October 5, 2023
Project Name:	Fusion Center Maturation	**E-mail:**	jeff.ly@pol.state.ma.us
Grant Program & FFY:	FSHSP20CFC 8000-4692 FFY2020	**Telephone:**	508-988-7081
Reported by:	Jeff Ly	**FAX:**	508-820-2165

Report Number	Reporting Period	Year	Report Due
Quarter _X_	July 1st – September 30th	2023	October 15th
Quarter ___	October 1st – December 31st	2023	January 15th
Quarter ___	January 1st – March 31st	2024	April 15th
Quarter ___	April 1st – June 30th	2023	July 15th

SUMMARY OF COSTS

Expense Category	Amended Budget	Expended This Quarter	Expended to Date	Obligated to Date	Balance	% Remaining
Salary	$48,570.00	$0.00	$48,570.00	$0.00	0.00	0%
Fringe	$20,640.79	$0.00	$20,640.79	$0.00	0.00	0%
Indirect	$8,524.05	$0.00	$8,524.05	$0.00	0.00	0%
Consultants/Contracts	$75,648.75	$0.00	$75,615.00	$0.00	33.75	0%
Travel	$5,896.72	$0.00	$5,226.47	$0.00	670.25	0%
Equipment	$407,000.00	$5,690.64	$404,217.33	$0.00	2,782.67	0%
Supplies	$0.00	$0.00	$0.00	$0.00	0.00	0%
Overtime	$0.00	$0.00	$0.00	$0.00	0.00	0%
Other (software, registrations, seminars)	$183,719.69	$0.00	$184,162.91	$0.00	(443.22)	0%
TOTAL	**$750,000.00**	**$5,690.64**	**$746,956.55**	**$0.00**	**$3,043.45**	0%

Reports must be submitted for every full or partial calendar quarter during the grant period regardless of spending activity.

Please send this report along with the Quarterly Financial Detail and Quarterly Progress Reports to:

Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720A

Boston, MA 02116
ATTN: Vicky Mboka-Boyer *via email*

Rebecca Rust
Authorized Signature (Blue ink please)

10/11/23
Date

Rebecca Rust
Print Name

Executive Office of Public Safety

Quarterly Financial Report (Detail for Expenditures)

Quarter Reporting Period (Choose From Cell Below) 7/1-9/30

Year Reporting Period (Choose From Cell Below) 2023

FSHSP20CFC -

Salary Please List all Employees charged to grant along with either: hours and rate, if paid hourly; or amount paid to employee for period from federal funds and a brief description, if salaried

Employee Name	Hrs/Unit	Rate/Amt	Description		Total
					-
					-
				Sub-Total:	**$0.00**

Fringe: Fringe costs must go by Federally approved rate, and base amount should easily be identified from this detailed report.

Employee Name	Approved Rate	Total dollars	Pay period		Total
				Sub-Total:	**$0.00**

Indirect: Indirect Rate must be a federally Negotiated and approved rate, and base amount should easily be identified from this detailed report.

Employee/Contracted Employee Name	Approved Rate	Total dollars			Total
				Sub-Total:	**$** -

Consultants/Contracts: Please list Name of Consultant or Entity contract is with, hours and rate of contract and a brief description. If total costs for quarter for any single contract exceed $5K, please provide invoices for

Company/Name	Hours	Rate	Description		Total
					-
					-
				Sub-Total:	**$0.00**

Travel: Please list each employee, cost of travel, description/purpose of travel, and the guidelines followed for reimbursement (Local, State, or Federal). Please include all receipts.

Employee Name	Cost	Guidelines	Purpose/Description	Total	Receipt Y/N
				Sub-Total:	$0.00

Piece of equipment	Unit Cost	Quantity	Description of Equipment	Total	Receipt
CDW-G Nvidia Jetson	[redacted]	[redacted]	Nvidia Jetson AGX Orin Dev Kit	$663.78	660.46
BSA - ALPR Brackets and Cables			16 Brackets and 5 Cables for ALPR	$5,030.18	5,030.18
			Sub-Total:		$5,690.64

Supplies: Please list supplies and computation basis for reimbursement request.

Item	Cost		Basis for Computation	Total	
			Sub-Total:		$0.00

Overtime

Employee Name	Hrs/Unit	Rate/Amt	Description	Total	
			Sub-Total:		$0.00

Other: Please list Item and Basis for Computation.

Item	Cost	Qty	Basis for Computation	Total	Receipt
				$0.00	-
			Sub-Total:		$0.00

Total

Total:* $5,690.64

2525

Reimbursable Grants Level 2

Menu

Department	Major Program	Program	Funding Profile	Funding Priority	Funding Line	Obligation Ceiling	Pre Encumbered	Encumbered	Total Expenses
POL	HSG2	FSHSP20CFC	FEDGRT	1	1	$750 000 00	$0 00	$0 00	$746 956 55

First Prev Next Last

Search

E pense Actuals

Pre Encumbered	$0.00	Obligation Ceiling	$750 000 00
Encumbered	$0 00	E penditure Ceiling	$750 000 00
Advances	$0.00	Uncommitted	$3 043 45
Accrued Expenses	$0 00	Une pended	$3 043 45
Cash E penses	$746,956.55	Back End plits	$0.00
Total Expenses	$746,956.55		
Charges	$0 00		

Revenue Actuals

Unbilled Earned Revenue	$0 00	Collected Earned Revenue	$746 956 55
Billed Earned Revenue	$0.00	Collected Unearned/De erred Revenue	$0 00
		Total Revenue	$746,956 55
		Revenue Credits	$0 00

Budgetary Amounts

Beginning Balance	$0 00	Revenue Beginning Balance	$0 00
Awarded	$750,000.00	Original Revenue Budget	$0 00
Amendments	$0 00	Revenue Amendments	$0 00
Trans er Out	$0.00	Current Revenue Budget	$0 00
Transfer In	$0 00	Unrecognized Revenue	($746 956 55)
Current Modi ied Budget	$750 000 00	Revenue Balance Forward	$0 00
Balance Forward	$0.00		

General In ormation

Department	POL	Name	FFY20 SHSP
Major Program	HSG2	tart Date	12/15/2020
Program	FSHSP20CFC	End Date	
Funding Pro ile	FEDGRT	Parent Dept	105
Funding Priority	1	Description	EXECUTIVE OFFICE OF PUBLIC SAFETY & HOMELAND SECURITY
Funding Line	1		
		Legal Cite	
		Active	☑

Top

Modified Budget Line Controls Previous Level

FSHSP20CFC
8000-4692

fiscal year	department	doc code	cash_expense amount	service_from date	service_to date	appropriation	object	object_name	vendor_customer code	legal name	program	acceptance date
2024	POL	EFT	$ 663.78	11-Jul-23	11-Jul-23	80004692	U07	Information Technology (IT) Equipment	VC6000240027	CDW GOVERNM	FSHSP20CFC	27-Jul-23
2024	POL	EFT	$ (3.32)	11-Jul-23	11-Jul-23	80004692	U07	Information Technology (IT) Equipment	VC6000240027	CDW GOVERNM	FSHSP20CFC	27-Jul-23
2024	POL	EFT	$ 5,030.18	01-Aug-23	01-Aug-23	80004692	U07	Information Technology (IT) Equipment	VC0000500765	BAY STATE ALAF	FSHSP20CFC	14-Sep-23

Total 9/30/2023 Expenditures 5,690.64 ✓

FSHSP20CFC
8000-4692

fiscal year	department	department_name	doc code	cash_expense amount	service_from date	service_to date	appropriation	object	object_name	vendor_customer code	legal name	program	acceptance date
2022	POL	DEPARTMENT OF	PRLNP	2,025.00	03-Aug-21	03-Aug-21	80004692	A01	Salaries Inclusive			FSHSP20CFC	03-Aug-21
2022	POL	DEPARTMENT OF	PRLNP	3,000.00	03-Aug-21	03-Aug-21	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	03-Aug-21
2022	POL	DEPARTMENT OF	PRLNP	1,830.00	17-Aug-21	17-Aug-21	80004692	A01	Salaries Inclusive			FSHSP20CFC	17-Aug-21
2022	POL	DEPARTMENT OF	PRLNP	3,000.00	17-Aug-21	17-Aug-21	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	17-Aug-21
2022	POL	DEPARTMENT OF	PRLNP	2,610.00	31-Aug-21	31-Aug-21	80004692	A01	Salaries Inclusive			FSHSP20CFC	31-Aug-21
2022	POL	DEPARTMENT OF	PRLNP	3,000.00	31-Aug-21	31-Aug-21	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	31-Aug-21
2022	POL	DEPARTMENT OF	CA	127.36			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	11-Sep-21
2022	POL	DEPARTMENT OF	CA	177.30			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	11-Sep-21
2022	POL	DEPARTMENT OF	CA	1,134.61			80004692	E16	Indirect Cost Recoupment			FSHSP20CFC	11-Sep-21
2022	POL	DEPARTMENT OF	CA	2,421.79			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	11-Sep-21
2022	POL	DEPARTMENT OF	PRLNP	1,680.00	14-Sep-21	14-Sep-21	80004692	A01	Salaries Inclusive			FSHSP20CFC	14-Sep-21
2022	POL	DEPARTMENT OF	PRLNP	3,000.00	14-Sep-21	14-Sep-21	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	14-Sep-21
2022	POL	DEPARTMENT OF	PRADJ	580.00	15-Sep-21	15-Sep-21	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	15-Sep-21
2022	POL	DEPARTMENT OF	PRADJ	3,035.00	15-Sep-21	15-Sep-21	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	15-Sep-21
2022	POL	DEPARTMENT OF	PRLNP	1,950.00	28-Sep-21	28-Sep-21	80004692	A01	Salaries Inclusive			FSHSP20CFC	28-Sep-21
2022	POL	DEPARTMENT OF	PRLNP	3,000.00	28-Sep-21	28-Sep-21	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	28-Sep-21
2022	POL	DEPARTMENT OF	CA	71.51			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	10-Oct-21
2022	POL	DEPARTMENT OF	CA	189.42			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	10-Oct-21
2022	POL	DEPARTMENT OF	CA	637.07			80004692	E16	Indirect Cost Recoupment			FSHSP20CFC	10-Oct-21
2022	POL	DEPARTMENT OF	CA	1,359.80			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	10-Oct-21
2022	POL	DEPARTMENT OF	PRLNP	550.00	12-Oct-21	12-Oct-21	80004692	B05	Conference, Training, Registration and Me			FSHSP20CFC	12-Oct-21
2022	POL	DEPARTMENT OF	PRLNP	1,974.46	12-Oct-21	12-Oct-21	80004692	B01	Other Out Of State Travel - INCLUSIVE AIR			FSHSP20CFC	12-Oct-21
2022	POL	DEPARTMENT OF	PRLNP	2,520.00	12-Oct-21	12-Oct-21	80004692	A01	Salaries Inclusive			FSHSP20CFC	12-Oct-21
2022	POL	DEPARTMENT OF	PRLNP	3,000.00	12-Oct-21	12-Oct-21	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	12-Oct-21
2022	POL	DEPARTMENT OF	PRLNP	2,850.00	26-Oct-21	26-Oct-21	80004692	A01	Salaries Inclusive			FSHSP20CFC	26-Oct-21
2022	POL	DEPARTMENT OF	PRLNP	3,000.00	26-Oct-21	26-Oct-21	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	26-Oct-21
2022	POL	DEPARTMENT OF	CA	105.79			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	07-Nov-21
2022	POL	DEPARTMENT OF	CA	118.20			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	07-Nov-21
2022	POL	DEPARTMENT OF	CA	942.44			80004692	E16	Indirect Cost Recoupment			FSHSP20CFC	07-Nov-21
2022	POL	DEPARTMENT OF	CA	2,011.60			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	07-Nov-21
2022	POL	DEPARTMENT OF	PRLNP	2,670.00	09-Nov-21	09-Nov-21	80004692	A01	Salaries Inclusive			FSHSP20CFC	09-Nov-21
2022	POL	DEPARTMENT OF	PRLNP	3,000.00	09-Nov-21	09-Nov-21	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	09-Nov-21
2022	POL	DEPARTMENT OF	PRLNP	2,685.00	23-Nov-21	23-Nov-21	80004692	A01	Salaries Inclusive			FSHSP20CFC	23-Nov-21
2022	POL	DEPARTMENT OF	PRLNP	3,000.00	23-Nov-21	23-Nov-21	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	23-Nov-21
2022	POL	DEPARTMENT OF	CA	105.49			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	04-Dec-21
2022	POL	DEPARTMENT OF	CA	118.20			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	04-Dec-21
2022	POL	DEPARTMENT OF	CA	939.80			80004692	E16	Indirect Cost Recoupment			FSHSP20CFC	04-Dec-21
2022	POL	DEPARTMENT OF	CA	2,005.98			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	04-Dec-21
2022	POL	DEPARTMENT OF	PRLNP	150.00	07-Dec-21	07-Dec-21	80004692	B05	Conference, Training, Registration and Me			FSHSP20CFC	07-Dec-21
2022	POL	DEPARTMENT OF	PRLNP	689.40	07-Dec-21	07-Dec-21	80004692	B01	Other Out Of State Travel - INCLUSIVE AIR			FSHSP20CFC	07-Dec-21
2022	POL	DEPARTMENT OF	PRLNP	2,040.00	07-Dec-21	07-Dec-21	80004692	A01	Salaries Inclusive			FSHSP20CFC	07-Dec-21
2022	POL	DEPARTMENT OF	PRLNP	3,000.00	07-Dec-21	07-Dec-21	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	07-Dec-21
2022	POL	DEPARTMENT OF	PRLNP	7.59	21-Dec-21	21-Dec-21	80004692	C98	Reimb Travel/Other Expenses CC Special C			FSHSP20CFC	21-Dec-21
2022	POL	DEPARTMENT OF	PRLNP	26.16	21-Dec-21	21-Dec-21	80004692	C98	Reimb Travel/Other Expenses CC Special C			FSHSP20CFC	21-Dec-21
2022	POL	DEPARTMENT OF	PRLNP	1,935.00	21-Dec-21	21-Dec-21	80004692	A01	Salaries Inclusive			FSHSP20CFC	21-Dec-21
2022	POL	DEPARTMENT OF	PRLNP	3,000.00	21-Dec-21	21-Dec-21	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	21-Dec-21
2022	POL	DEPARTMENT OF	PRLNP	1,035.00	04-Jan-22	04-Jan-22	80004692	A01	Salaries Inclusive			FSHSP20CFC	04-Jan-22
2022	POL	DEPARTMENT OF	PRLNP	3,000.00	04-Jan-22	04-Jan-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	04-Jan-22
2022	POL	DEPARTMENT OF	CA	78.31			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	15-Jan-22
2022	POL	DEPARTMENT OF	CA	118.20			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	15-Jan-22
2022	POL	DEPARTMENT OF	CA	697.61			80004692	E16	Indirect Cost Recoupment			FSHSP20CFC	15-Jan-22
2022	POL	DEPARTMENT OF	CA	1,489.04			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	15-Jan-22
2022	POL	DEPARTMENT OF	PRLNP	2,055.00	18-Jan-22	18-Jan-22	80004692	A01	Salaries Inclusive			FSHSP20CFC	18-Jan-22
2022	POL	DEPARTMENT OF	PRLNP	3,000.00	18-Jan-22	18-Jan-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	18-Jan-22
2022	POL	DEPARTMENT OF	PRLNP	2,595.00	01-Feb-22	01-Feb-22	80004692	A01	Salaries Inclusive			FSHSP20CFC	01-Feb-22
2022	POL	DEPARTMENT OF	PRLNP	3,000.00	01-Feb-22	01-Feb-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	01-Feb-22
2022	POL	DEPARTMENT OF	CA	60.87			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	05-Feb-22
2022	POL	DEPARTMENT OF	CA	118.20			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	05-Feb-22
2022	POL	DEPARTMENT OF	CA	542.30			80004692	E16	Indirect Cost Recoupment			FSHSP20CFC	05-Feb-22
2022	POL	DEPARTMENT OF	CA	1,157.51			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	05-Feb-22
2022	POL	DEPARTMENT OF	PRLNP	1,920.00	15-Feb-22	15-Feb-22	80004692	A01	Salaries Inclusive			FSHSP20CFC	15-Feb-22
2022	POL	DEPARTMENT OF	PRLNP	3,000.00	15-Feb-22	15-Feb-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	15-Feb-22
2022	POL	DEPARTMENT OF	PRLNP	175.21	01-Mar-22	01-Mar-22	80004692	B02	In-State Travel			FSHSP20CFC	01-Mar-22
2022	POL	DEPARTMENT OF	PRLNP	550.00	01-Mar-22	01-Mar-22	80004692	B05	Conference, Training, Registration and Me			FSHSP20CFC	01-Mar-22
2022	POL	DEPARTMENT OF	PRLNP	1,260.00	01-Mar-22	01-Mar-22	80004692	A01	Salaries Inclusive			FSHSP20CFC	01-Mar-22
2022	POL	DEPARTMENT OF	PRLNP	1,598.08	01-Mar-22	01-Mar-22	80004692	B01	Other Out Of State Travel - INCLUSIVE AIR			FSHSP20CFC	01-Mar-22
2022	POL	DEPARTMENT OF	PRLNP	3,000.00	01-Mar-22	01-Mar-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	01-Mar-22
2022	POL	DEPARTMENT OF	CA	88.95			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	05-Mar-22
2022	POL	DEPARTMENT OF	CA	118.20			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	05-Mar-22
2022	POL	DEPARTMENT OF	CA	792.38			80004692	E16	Indirect Cost Recoupment			FSHSP20CFC	05-Mar-22
2022	POL	DEPARTMENT OF	CA	1,691.32			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	05-Mar-22
2022	POL	DEPARTMENT OF	EFT	136.00	13-Jan-22	30-Jun-22	80004692	U10	Information Tech (IT) Equipment Mainten	VC6000227588	SHI INTERNATIO	FSHSP20CFC	11-Mar-22
2022	POL	DEPARTMENT OF	PRLNP	2,250.00	15-Mar-22	15-Mar-22	80004692	A01	Salaries Inclusive			FSHSP20CFC	15-Mar-22
2022	POL	DEPARTMENT OF	PRLNP	3,000.00	15-Mar-22	15-Mar-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	15-Mar-22
2022	POL	DEPARTMENT OF	PRLNP	154.00	29-Mar-22	29-Mar-22	80004692	B05	Conference, Training, Registration and Me			FSHSP20CFC	29-Mar-22
2022	POL	DEPARTMENT OF	PRLNP	3,000.00	29-Mar-22	29-Mar-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	29-Mar-22
2022	POL	DEPARTMENT OF	PRLNP	3,000.00	29-Mar-22	29-Mar-22	80004692	A01	Salaries Inclusive			FSHSP20CFC	29-Mar-22
2022	POL	DEPARTMENT OF	CA	128.25			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	09-Apr-22
2022	POL	DEPARTMENT OF	CA	177.30			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	09-Apr-22
2022	POL	DEPARTMENT OF	CA	1,142.51			80004692	E16	Indirect Cost Recoupment			FSHSP20CFC	09-Apr-22
2022	POL	DEPARTMENT OF	CA	2,438.65			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	09-Apr-22
2022	POL	DEPARTMENT OF	PRLNP	2,820.00	12-Apr-22	12-Apr-22	80004692	A01	Salaries Inclusive			FSHSP20CFC	12-Apr-22
2022	POL	DEPARTMENT OF	PRLNP	3,000.00	12-Apr-22	12-Apr-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	12-Apr-22
2022	POL	DEPARTMENT OF	PRLNP	2,325.00	26-Apr-22	26-Apr-22	80004692	A01	Salaries Inclusive			FSHSP20CFC	26-Apr-22
2022	POL	DEPARTMENT OF	PRLNP	3,000.00	26-Apr-22	26-Apr-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	26-Apr-22
2022	POL	DEPARTMENT OF	CA	101.36			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	07-May-22
2022	POL	DEPARTMENT OF	CA	118.20			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	07-May-22
2022	POL	DEPARTMENT OF	CA	902.95			80004692	E16	Indirect Cost Recoupment			FSHSP20CFC	07-May-22
2022	POL	DEPARTMENT OF	CA	1,927.32			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	07-May-22
2022	POL	DEPARTMENT OF	PRLNP	1,905.00	10-May-22	10-May-22	80004692	A01	Salaries Inclusive			FSHSP20CFC	10-May-22

2022	POL	DEPARTMENT OF	PRLNP	3,000.00	10-May-22	10-May-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	10-May-22
2022	POL	DEPARTMENT OF	PRLNP	2,130.00	24-May-22	24-May-22	80004692	A01	Salaries Inclusive			FSHSP20CFC	24-May-22
2022	POL	DEPARTMENT OF	PRLNP	3,000.00	24-May-22	24-May-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	24-May-22
2022	POL	DEPARTMENT OF	PRLNP	480.00	07-Jun-22	07-Jun-22	80004692	A01	Salaries Inclusive			FSHSP20CFC	07-Jun-22
2022	POL	DEPARTMENT OF	PRLNP	3,000.00	07-Jun-22	07-Jun-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	07-Jun-22
2022	POL	DEPARTMENT OF	CA	79.49			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	11-Jun-22
2022	POL	DEPARTMENT OF	CA	118.20			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	11-Jun-22
2022	POL	DEPARTMENT OF	CA	708.14			80004692	E16	Indirect Cost Recoupment			FSHSP20CFC	11-Jun-22
2022	POL	DEPARTMENT OF	CA	1,511.51			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	11-Jun-22
2022	POL	DEPARTMENT OF	EFT	22,880.00	09-May-22	09-May-22	80004692	U03	Software & Information Technology Licens	VC6000227588	SHI INTERNATIO	FSHSP20CFC	13-Jun-22
2022	POL	DEPARTMENT OF	PRLNP	3,000.00	21-Jun-22	21-Jun-22	80004692	C23	Management, Business Professionals & Ad			FSHSP20CFC	21-Jun-22
2022	POL	DEPARTMENT OF	PRLNP	55.57	06-Jul-22	06-Jul-22	80004692	B02	In-State Travel			FSHSP20CFC	06-Jul-22
2022	POL	DEPARTMENT OF	CA	9.46			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	09-Jul-22
2022	POL	DEPARTMENT OF	CA	84.24			80004692	E16	Indirect Cost Recoupment			FSHSP20CFC	09-Jul-22
2022	POL	DEPARTMENT OF	CA	118.20			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	09-Jul-22
2022	POL	DEPARTMENT OF	CA	179.81			80004692	D09	Fringe Benefit Cost Recoupment			FSHSP20CFC	09-Jul-22
2023	POL	DEPARTMENT OF	EFT	(5,094.00)	06-Apr-23	06-Apr-23	80004692	K10	Law Enforcement & Security Equipment	VC0000506451	BAIN COR INC	FSHSP20CFC	14-Apr-23
2023	POL	DEPARTMENT OF	EFT	254,700.00	06-Apr-23	06-Apr-23	80004692	K10	Law Enforcement & Security Equipment	VC0000506451	BAIN COR INC	FSHSP20CFC	14-Apr-23
2023	POL	DEPARTMENT OF	EFT	160,442.91	23-Mar-23	23-Mar-23	80004692	U12	Information Tech (IT) cloud services	VC6000239916	INSIGHT PUBLIC	FSHSP20CFC	04-May-23
2023	POL	DEPARTMENT OF	EFT	(3,039.20)	03-May-23	03-May-23	80004692	U07	Information Technology (IT) Equipment	VC0000500765	BAY STATE ALAR	FSHSP20CFC	12-May-23
2023	POL	DEPARTMENT OF	EFT	151,959.89	03-May-23	03-May-23	80004692	U07	Information Technology (IT) Equipment	VC0000500765	BAY STATE ALAR	FSHSP20CFC	12-May-23
2024	POL	DEPARTMENT OF	EFT	663.78	11-Jul-23	11-Jul-23	80004692	U07	Information Technology (IT) Equipment	VC6000240027	CDW GOVERNM	FSHSP20CFC	27-Jul-23
2024	POL	DEPARTMENT OF	EFT	(3.32)	11-Jul-23	11-Jul-23	80004692	U07	Information Technology (IT) Equipment	VC6000240027	CDW GOVERNM	FSHSP20CFC	27-Jul-23
2024	POL	DEPARTMENT OF	EFT	5,030.18	01-Aug-23	01-Aug-23	80004692	U07	Information Technology (IT) Equipment	VC0000500765	BAY STATE ALAR	FSHSP20CFC	14-Sep-23

Total ALL Expenditures to 9/30/2023 746,956.55 ✓

⚠ This transaction exceeds the unexpended funds for this budget. (W0030)

Electronic Funds Transfer(EFT) **Dept:** CTR **ID:** DISB0727230000102607 **Ver.:** 1 **Function:** New **Phase:** Final **Modified by** sa , 07/27/2023

Vendor **Total Lines:** 1 **Vendor Line:** 1 **Vendor Customer:** VC6000240027 **Legal Name:** CDW GOVERNMENT LLC

Vendor Line	Vendor Customer	Legal Name	Line Amount	County Name
1	VC6000240027	CDW GOVERNMENT LLC	$12,537.27	

From 1 to 1 Total: 1

General Information

Vendor Customer:
VC6000240027
Legal Name:
CDW GOVERNMENT LLC
Alias/DBA:

Address Code:
AD001
Address Line 1:
75 REMITTANCE DR STE 1515
Address Line 2:

City:
CHICAGO
State:
IL
Zip:
60675
Country:
USA
County:

Vendor Contact ID:

Principal Contact:
NONE PROVIDED
Phone:
NONE PROVIDED
Phone Extension:

Email Address:

Fax Number:

Fax Extension:

Web Address http://:

Line Amount:
$12,537.27

Additional Information

Taxpayer ID Number:

Taxpayer ID Number Type:

Parent Account:
VC6000240027
Default Disbursement Format:
CTX
Disbursement Category:
100
EFT Status:
Eligible for EFT

Parent Account:
Yes
Valid Address:
No
Prevent New Spending:
No
Restricted Use:
No
Misc. Account:
No
Held Payment:
No
Vendor Single Check:
No
Third Party Only:
No
Third Party Vendor:
No
Third Party Customer:
No
Require Tax ID:
No
Internal Account:
No
Bill Parent:
No

This transaction exceeds the unexpended funds for this budget. (W0030)

Electronic Funds Transfer(EFT) **Dept:** CTR **ID:** DISB0727230000102607 **Ver.:** 1 **Function:** New **Phase:** Final **Modified by** sa , 07/27/2023

Accounting **Total Lines:** 8 **Accounting Line:** 7 **Line Amount:** $663.78

	Accounting Line	Line Amount	Line Closed Amount	Check Amount	Event Type
	1	$1,104.34	$0.00	$1,104.34	DI02
	2	$1,104.34	$0.00	$1,104.34	DI02
	3	$1,104.34	$0.00	$1,104.34	DI02
	4	$4,417.36	$0.00	$4,417.36	DI02
	5	$13.22	$0.00	$13.22	DI02
	6	$199.99	$0.00	$199.99	DI02
	7	$663.78	$0.00	$660.46	DI02
	8	$3,929.90	$0.00	$3,929.90	DI02

From 1 to 8 Total: 8

General Information

Event Type:
DI02
Accounting Template:

Check Description:
INVOICE KP68362
Line Description:
(1) NVIDIA Jetson AGX Orin Dev Kit, MFG part# 945-13766-0007-000
Check Amount:
$660.46
Vendor Invoice Number:
KP68362
Vendor Invoice Line Number:
1
Vendor Invoice Date:
07/18/2023
Invoice Received Date:
07/20/2023
Remittance Advice Transmission Mode:

Budget FY:
2024
Fiscal Year:
2024
Period:
1
Interest Ineligible Flag:

Interest Calculated or Bypassed:

Calculated Interest Amount:

Service From Date:
07/11/2023
Service To Date:
07/11/2023
Warrant Number:
M01
Replacement:

PY Accrual/Clearing %:

Procurement Folder:
7858527
Procurement Type ID:
1
Procurement Type:
Unclassified

Reference

Ref Doc Code:
PRC
Ref Doc Dept:
POL
Ref Doc ID:
PVPOL721424201CDWUXX
Ref Vendor Line:
1
Ref Commodity Line:
1
Ref Accounting Line:
1
Ref Type:
Final

PO/RQ Document Code:
PC
PO/RQ Document Department:
POL
PO/RQ Document ID:
2024CDWG1U07POL20805
PO/RQ Document Vendor Line:
1
PO/RQ Commodity Line:
1
PO/RQ Accounting Line:
1

Fixed Asset Intent Reference

FN Document Code:

FN Document Department:

FN Document ID:

Fund Accounting

Fund:
0100
Sub Fund:
0000
Department:
POL
Unit:
7214
Sub Unit:

Appr Unit:
80004692

Object:
U07
Sub Object:

Revenue:

Sub Revenue:

BSA:

Sub BSA:

OBSA:

Sub OBSA:

Dept Object:

Dept Revenue:

Detail Accounting

Location:

Sub Location:

Activity:

Sub Activity:

Function:

Sub Function:

Reporting:

Sub Reporting:

Task:

Sub Task:

Task Order:

Major Program:
HSG2
Program:
FSHSP20CFC
Phase:

Program Period:
2005

Additional Amounts

Line Amount:
$663.78

Intercept Line Amount:
$0.00

Line Closed Amount:
$0.00

Discount Line Amount:
$3.32
Penalty Line Amount:
$0.00
Interest Line Amount:
$0.00
Backup Withholding Amount:
$0.00
Contract Withholding Amount:
$0.00

Default Intercept Fee Amount:
$0.00
Supplementary Intercept Fee Amount:
$0.00
Retainage Line Amount:
$0.00
Freight Amount:
$0.00
Use Tax amount:
$0.00
Tax Amount:
$0.00

Line Closed Date:

Additional Information

Contact (name):
DEPARTMENT OF STATE POLICE
Contact Location:
470 Worcester Road
Contact Telephone:
(508) 820-2141
Contact Telephone Extension:

Special Instructions Code:

Disbursement Frequency:
Daily
Advance Type:

Dyna Bank:

1042-S Tax Rate:

Scheduling Reason Code:

Discount Term 1 Applied:

Discount Term 2 Applied:

Discount Term 3 Applied:

Discount Term 4 Applied:

2532

View All 1 of 6 | Document validated successfully

Pymt Request-CommodityBased(PRC) **Dept:** POL **ID:** PVPOL721424201CDWUXX **Ver.:** 1 **Function:** New **Phase:** Draft Finance

Document Navigator 0/2023

Vendor **Total Lines:** 1 **Vendor Line:** 1 **Vendor Customer:** VC6000240027 **Legal Name:** CDW GOVERNMENT LLC

	Vendor Line	Vendor Customer	Legal Name	Line Amount		
	1	VC6000240027	CDW GOVERNMENT LLC	663.78		

From 1 to 1 Total: 1

Unit #7214 8000-4692 FSHSP20CFC

General Information

Vendor Customer: VC6000240027
Legal Name: CDW GOVERNMENT LLC
Alias/DBA:
Address Code: AD001
Address 1: 75 REMITTANCE DR STE 1
Address 2:
City: CHICAGO
State: Illinois
Zip Code: 60675
Country: USA
County:

Vendor Contact ID:
Vendor Contact Name: NONE PROVIDED
Vendor Contact Phone: NONE PROVIDED
Vendor Contact Phone Ext.:
Vendor Contact Email:
Fax:
Fax Extension:
Web Address http://:
Taxpayer ID Number:
Taxpayer ID Type:
Merchant ID:
Tax Profile:
Received Service From Date:
Received Service To Date:

Disbursement Options

Disbursement Type: EFT
Disbursement Format: CTX
Scheduled Payment Date: 07/27/2023
Disbursement Priority: 99
Single Payment: ☐
Pay Third Party: ☐
On-line Disbursement Rqst: ☐
EFT Status: Eligible for EFT

Handling Code:
Disbursement Category: 100

Invoice Information

Invoice Doc Code:
Invoice Doc Dept:
Invoice Doc ID:

Vendor Invoice Number:
Vendor Invoice Date:
Tracking Date:

2533 07/20/2023

Invoice Acceptance/Sign-Off Date:

Agreement Reference

Agreement Ref Code:

Agreement Ref Vendor Line:

Agreement Ref Dept:

Agreement Ref ID:

Discount Terms

Days 1: 9	**Percent 1:** 0.5000	**Discount Always 1:** ☐
Days 2:	**Percent 2:**	**Discount Always 2:** ☐
Days 3:	**Percent 3:**	**Discount Always 3:** ☐
Days 4:	**Percent 4:**	**Discount Always 4:** ☐

2534

REMIT PAYMENT TO:

CDW Government
75 Remittance Drive, Suite 1515
Chicago, IL 60675-1515

RETURN SERVICE REQUESTED

INVOICE

ACH INFORMATION:
THE NORTHERN TRUST
50 SOUTH LASALLE STREET
CHICAGO, IL 60675
ROUTING
ACCOUNT
ACCOUNT

E-mail Remittance To: gachremittance@cdw.com
G L. c. 4.sec. 7 cl.26 (n)(security)

INVOICE NUMBER	INVOICE DATE	CUSTOMER NUMBER
KP68362	07/08/23	4668629
SUBTOTAL	**SHIPPING**	**SALES TAX**
$663.78	$0.00	$0.00
DUE DATE		**AMOUNT DUE**
08/07/23		**$663.78**

EOPPS MASSACHUSETTS STATE POLICE
ACCOUNTS PAYABL
470 WORCESTER RD
FRAMINGHAM MA 01702-5309

CDW Government
75 Remittance Drive
Suite 1515
Chicago, IL 60675-1515

PLEASE RETURN THIS PORTION WITH YOUR PAYMENT

INVOICE DATE	INVOICE NUMBER	PAYMENT TERMS	DUE DATE
07/08/23	KP68362	Net 30 Days	08/07/23
ORDER DATE	**SHIP VIA**	**PURCHASE ORDER NUMBER**	**CUSTOMER NUMBER**
06/13/23	DROP SHIP-GROUND	2023CDWG1U07POL20805	4668629

ITEM NUMBER	DESCRIPTION	QTY ORD	QTY SHIP	QTY B/O	UNIT PRICE	TOTAL
7449972	NVIDIA JETSON AGX ORIN DEV KIT Manufacturer Part Number: 945-13766-0007-000	1	1	0	663.78	663.78

Invoice Receipt date JUL 18 2023

"The equipment, goods or services for which this payment is made were received on 7/11/23"

certified by Stephani Peters

signature date 7/19/2023

Received by:

Sgt. N. Pack #3680

Signed date: 7/18/2023

GO GREEN!

CDW is happy to announce that paperless billing is now available! If you would like to start receiving your invoices as an emailed PDF, please email CDW at paperlessbilling@cdw.com. Please include your Customer number or an Invoice number in your email for faster processing.

REDUCE PROCESSING COSTS AND ELIMINATE THE HASSLE OF PAPER CHECKS!

Begin transmitting your payments electronically via ACH using CDW's bank and remittance information located at the top of the attached payment coupon. Email credit@cdw.com with any questions.

ACCOUNT MANAGER	SHIPPING ADDRESS:
DAN PALMIERI 203-851-7223 dan.palmieri@cdwg.com	EOPPS MASSACHUSETTS STATE POLICE NOAH PACK 470 WORCESTER RD FRAMINGHAM MA 01702-5309
SALES ORDER NUMBER	
NKTN604	

SUBTOTAL	$663.78
SHIPPING	$0.00
SALES TAX	$0.00
AMOUNT DUE	$663.78

Cage Code Number 1KH72
DUNS Number 02-615-7235
Unique Entity ID (SAM): PHZDZ8SJ5CM1
ISO 9001 and ISO 14001 Certified
CDW GOVERNMENT FEIN 36-4230110

HAVE QUESTIONS ABOUT YOUR ACCOUNT?
PLEASE EMAIL US AT credit@cdw.com
VISIT US ON THE INTERNET AT www.cdwg.com

2535

REMIT PAYMENT TO:

CDW Government
75 Remittance Drive, Suite 1515
Chicago, IL 60675-1515

RETURN SERVICE REQUESTED

INVOICE

ACH INFORMATION:
THE NORTHERN TRUST
50 SOUTH LASALLE STREET
CHICAGO, IL 60675

E-mail Remittance To: gschremittance@cdw.com
ROUTING NO.: 071000152
ACCOUNT NAME: CDW GOVERNMENT
ACCOUNT NO.: 91067

INVOICE NUMBER	INVOICE DATE	CUSTOMER NUMBER
KP68362	07/08/23	4668629
SUBTOTAL	**SHIPPING**	**SALES TAX**
$663.78	$0.00	$0.00
DUE DATE		**AMOUNT DUE**
08/07/23		$663.78

2 1 SP 0.600 E0002X I004 D11457253735 82 P9789327 0001:0001

EOPPS MASSACHUSETTS STATE POLICE
ACCOUNTS PAYABL
470 WORCESTER RD
FRAMINGHAM MA 01702-5309

CDW Government
75 Remittance Drive
Suite 1515
Chicago, IL 60675-1515

PLEASE RETURN THIS PORTION WITH YOUR PAYMENT

INVOICE DATE	INVOICE NUMBER	PAYMENT TERMS	DUE DATE
07/08/23	KP68362	Net 30 Days	08/07/23
ORDER DATE	**SHIP VIA**	**PURCHASE ORDER NUMBER**	**CUSTOMER NUMBER**
06/13/23	DROP SHIP-GROUND	2023CDWG1U07POL20805	4668629

ITEM NUMBER	DESCRIPTION	QTY ORD	QTY SHIP	QTY B/O	UNIT PRICE	TOTAL
7449972	NVIDIA JETSON AGX ORIN DEV KIT Manufacturer Part Number: 945-13766-0007-000	1	1	0	663.78	663.78

RECEIVED
JUL 18 2023
State Police Finance Unit

GO GREEN!

CDW is happy to announce that paperless billing is now available! If you would like to start receiving your invoices as an emailed PDF, please email CDW at paperlessbilling@cdw.com. Please include your Customer number or an Invoice number in your email for faster processing.

REDUCE PROCESSING COSTS AND ELIMINATE THE HASSLE OF PAPER CHECKS!

Begin transmitting your payments electronically via ACH using CDW's bank and remittance information located at the top of the attached payment coupon. Email credit@cdw.com with any questions.

ACCOUNT MANAGER	SHIPPING ADDRESS:		
DAN PALMIERI 203-851-7223 dan.palmieri@cdwg.com	EOPPS MASSACHUSETTS STATE POLICE NOAH PACK 470 WORCESTER RD FRAMINGHAM MA 01702-5309	SUBTOTAL	$663.78
		SHIPPING	$0.00
SALES ORDER NUMBER		SALES TAX	$0.00
NKTN604		AMOUNT DUE	$663.78

Cage Code Number 1KH72
DUNS Number 02-615-7235
Unique Entity ID (SAM): PHZDZ8SJ5CM1
ISO 9001 and ISO 14001 Certified
CDW GOVERNMENT FEIN 36-4230110

HAVE QUESTIONS ABOUT YOUR ACCOUNT?
PLEASE EMAIL US AT credit@cdw.com
VISIT US ON THE INTERNET AT www.cdwg.com

0001:0001

2536

FSHSP20GC
Unit # 7214
8000-4692

CDW•G PEOPLE WHO GET IT

Thank you for choosing CDW. We have received your quote.

Hardware Software Services IT Solutions Brands Research Hub

Review and Complete Purchase

GUSTAV PEARSON,

Thank you for considering CDW•G for your technology needs. The details of your quote are below. **If you are an eProcurement or single sign on customer, please log into your system to access the CDW site.** You can search for your quote to retrieve and transfer back into your system for processing.

For all other customers, click below to convert your quote to an order.

Approved by:

Sgt. N. Pack #3680

Convert Quote to Order

QUOTE #	QUOTE DATE	QUOTE REFERENCE	CUSTOMER #	GRAND TOTAL
NJTJ895	5/10/2023	NJTJ895	4666629	$663.78

QUOTE DETAILS

ITEM	QTY	CDW#	UNIT PRICE	EXT. PRICE
NVIDIA JETSON AGX ORIN DEV KIT Mfg. Part#: 945-13766-0007-000 Contract: MARKET	1	7449972	$663.78	$663.78

Received on 7/11/2023 by:

Sgt. N. Pack #3680

SUBTOTAL	$663.78
SHIPPING	$0.00
SALES TAX	$0.00
GRAND TOTAL	$663.78

PURCHASER BILLING INFO	DELIVER TO
Billing Address: EOPPS MASSACHUSETTS STATE POLICE ACCOUNTS PAYABL 470 WORCESTER RD FRAMINGHAM, MA 01702-5309 Phone: (508) 988-7407 Payment Terms: Net 30 Days-Govt State/Local	Shipping Address: EOPPS MASSACHUSETTS STATE POLICE NOAH PACK 470 WORCESTER RD FRAMINGHAM, MA 01702-5309 Phone: (508) 988-7407 Shipping Method: DROP SHIP-GROUND
	Please remit payments to: CDW Government 75 Remittance Drive Suite 1515 Chicago, IL 60675-1515

Sales Contact Info

Dan Palmieri | (855) 822-4918 | dan.palmieri@cdwg.com

Need Help?

My Account | Support | Call 800.800.4239

This transaction exceeds the unexpended funds for this budget. (W0030)

Electronic Funds Transfer(EFT) **Dept:** CTR **ID:** DISB0914230000257284 **Ver.:** 1 **Function:** New **Phase:** Final **Modified by** sa , 09/14/2023

Vendor **Total Lines:** 1 **Vendor Line:** 1 **Vendor Customer:** VC0000500765 **Legal Name:** BAY STATE ALARM SECURITY INC

	Vendor Line	Vendor Customer	Legal Name	Line Amount	County Name
	1	VC0000500765	BAY STATE ALARM SECURITY INC	$5,030.18	

From 1 to 1 Total: 1

General Information

Vendor Customer:
VC0000500765
Legal Name:
BAY STATE ALARM SECURITY INC
Alias/DBA:
BSA SECURITY INTEGRATORS
Address Code:
AD001
Address Line 1:
462 PLEASANT ST
Address Line 2:

City:
MARLBOROUGH
State:
MA
Zip:
01752-1127
Country:
USA
County:

Vendor Contact ID:

Principal Contact:
JAMES P. MCSTAY
Phone:
508-485-1174
Phone Extension:
112
Email Address:

Fax Number:

Fax Extension:

Web Address http://:

Line Amount:
$5,030.18

Additional Information

Taxpayer ID Number:

Taxpayer ID Number Type:

Parent Account:
VC0000500765
Default Disbursement Format:
CTX
Disbursement Category:
100
EFT Status:
Eligible for EFT

Parent Account:
Yes
Valid Address:
No
Prevent New Spending:
No
Restricted Use:
No
Misc. Account:
No
Held Payment:
No
Vendor Single Check:
No
Third Party Only:
No
Third Party Vendor:
No
Third Party Customer:
No
Require Tax ID:
No
Internal Account:
No
Bill Parent:
No

This transaction exceeds the unexpended funds for this budget. (W0030)

Electronic Funds Transfer(EFT) **Dept:** CTR **ID:** DISB0914230000257284 **Ver.:** 1 **Function:** New **Phase:** Final **Modified by** sa , 09/14/2023

Accounting **Total Lines:** 1 **Accounting Line:** 1 **Line Amount:** $5,030.18

Accounting Line	Line Amount	Line Closed Amount	Check Amount	Event Type
1	$5,030.18	$0.00	$5,030.18	DI02

From 1 to 1 Total: 1

General Information

Event Type:
DI02
Accounting Template:

Check Description:
INVOICE 11500

Line Description:
(8) 3 AXIS P52X Brackets(8) Urban Traffic Light Bracket(5) Single Ethernet Cable (1) Mounthard
Check Amount:
$5,030.18
Vendor Invoice Number:
11500
Vendor Invoice Line Number:
1
Vendor Invoice Date:
08/03/2023
Invoice Received Date:
08/29/2023
Remittance Advice Transmission Mode:

Budget FY:
2024
Fiscal Year:
2024
Period:
3
Interest Ineligible Flag:

Interest Calculated or Bypassed:

Calculated Interest Amount:

Service From Date:
08/01/2023
Service To Date:
08/01/2023
Warrant Number:
M03
Replacement:

PY Accrual/Clearing %:

Procurement Folder:
7904120
Procurement Type ID:
1
Procurement Type:
Unclassified

Reference

Ref Doc Code:
PRC
Ref Doc Dept:
POL
Ref Doc ID:
PVPOL721424241BSASIX
Ref Vendor Line:
1
Ref Commodity Line:
1
Ref Accounting Line:
1
Ref Type:
Final

PO/RQ Document Code:
PC
PO/RQ Document Department:
POL
PO/RQ Document ID:
2024BSASIU07POL20806
PO/RQ Document Vendor Line:
1
PO/RQ Commodity Line:
1
PO/RQ Accounting Line:
1

Fixed Asset Intent Reference

FN Document Code:

FN Document Department:

FN Document ID:

Fund Accounting

Fund:
0100
Sub Fund:
0000
Department:
POL
Unit:
7214
Sub Unit:
Appr Unit:
80004692

Object:
U07
Sub Object:
Revenue:
Sub Revenue:
BSA:
Sub BSA:

OBSA:
Sub OBSA:
Dept Object:
Dept Revenue:

Detail Accounting

Location:
Sub Location:
Activity:
Sub Activity:
Function:
Sub Function:

Reporting:
Sub Reporting:
Task:
Sub Task:
Task Order:

Major Program:
HSG2
Program:
FSHSP20CFC
Phase:
Program Period:
2005

Additional Amounts

Line Amount:
$5,030.18
Discount Line Amount:
$0.00
Penalty Line Amount:
$0.00
Interest Line Amount:
$0.00
Backup Withholding Amount:
$0.00
Contract Withholding Amount:
$0.00

Intercept Line Amount:
$0.00
Default Intercept Fee Amount:
$0.00
Supplementary Intercept Fee Amount:
$0.00
Retainage Line Amount:
$0.00
Freight Amount:
$0.00
Use Tax amount:
$0.00

Line Closed Amount:
$0.00
Line Closed Date:

Tax Amount:
$0.00

Additional Information

Contact (name):
DEPARTMENT OF STATE POLICE
Contact Location:
470 Worcester Road
Contact Telephone:
(508) 820-2141
Contact Telephone Extension:

Special Instructions Code:

Disbursement Frequency:
Daily
Advance Type:

Dyna Bank:

1042-S Tax Rate:

Scheduling Reason Code:

Discount Term 1 Applied:

Discount Term 2 Applied:

Discount Term 3 Applied:

Discount Term 4 Applied:

2510

BSASi Security Integrators

Bay State Alarm Security, Inc.
462 Pleasant Street, Marlboro, MA 01752
Phone 508-485-1174 Fax 508-624-6568

GSA Advantage!

INVOICE

Invoice Number: 11500
Invoice Date: Aug 1, 2023
Page: 1

Bill To:

Massachusetts State Police General
470 Worcester Road
Framingham, MA 01702

Job:

PO 2023BSASIU07POL20806

Customer ID	Customer PO	Payment Terms	
MA State Police	2023BSASIU07POL20806	Net 30 Days	
Service Tech ID	**Job Ticket ID**	**Date of Service**	**Due Date**
			8/31/23

Quantity	Item	Description	Unit Price	Amount
8.00	Ea	FA3520000001 3 Axis P52	191.88	1,535.04
8.00	Ea	HC3928401A	254.63	2,037.04
5.00	Ea	HC350242L010	282.11	1,410.55
1.00	Ea	Mounting Hardware brackets bolts washer nuts	47.55	47.55

Invoice Receipt date AUG 0 3 2023

"The equipment, goods or services for which this payment is made were received on Aug 1/23

certified by [signature] #3731

signature date 8/29/23

Subtotal	5,030.18 ✓
Sales Tax	
Total Invoice Amount	5,030.18
Payment/Credit Applied	
TOTAL	**5,030.18**

Check/Credit Memo No:

GSA Advantage!

SDVOSB

2541

BSASi Security Integrators

SDVOSB Disabled Veteran Owned Small Business Service CVE

Packing List

MSP050823.1

Bay State Alarm Security, Inc. * 462 Pleasant Street * Marlboro, MA 01752 Ph 508-485-1174 Fax 508-624-6568

To:	**Massachusetts State Police**	**Date: July 31, 202**
	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 Neology Brackets and Adapters
Re:	IRIS Bracket Items	

#	QTY	U/M	DESCRIPTION
1.	[redacted]	Ea	FA3520000001 – 3 AXIS P52X BRACKETS
2.		Ea	HC3928401A – URBAN TRAFFIC LIGHT BRACKET
3.		Ea	HC350242L010 – SINGLE ETHERNET CABLE (10M) FOR 525
4.		Ea	MOUNTING HARDWARE FOR BRACKETS: BOLTS, WASHERS, & NUTS
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			

GSA Advantage!

Signature Please Sgt. Ryan Walsh #3731 8/29/23

Grant Program Spending Report

Appropriation	Program	BFY	Doc_ID_Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
Dept: POL										
80004692	HOMELAND SECURITY II									
FSHSP20CFC	COMMONWEALTH FUSION CENTER									
		2022								
object_class	AA									
A01	Salaries: Inclusive									
PREXPPOL			EMPL	020210731148138		$2,025.00			8/3/2021	8/3/2021	8/3/2021
PREXPPOL			EMPL	020210814141338		$1,830.00			8/17/2021	8/17/2021	8/17/2021
PREXPPOL			EMPL	020210828150808		$2,610.00			8/31/2021	8/31/2021	8/31/2021
PREXPPOL			EMPL	020210911142238		$1,680.00			9/14/2021	9/14/2021	9/14/2021
PREXPPOL			EMPL	020210925147338		$1,950.00			9/28/2021	9/28/2021	9/28/2021
PREXPPOL			EMPL	020211009159078		$2,520.00			10/12/2021	10/12/2021	10/12/2021
PREXPPOL			EMPL	020211023149008		$2,850.00			10/26/2021	10/26/2021	10/26/2021
PREXPPOL			EMPL	020211106154318		$2,670.00			11/9/2021	11/9/2021	11/9/2021
PREXPPOL			EMPL	020211120148528		$2,685.00			11/23/2021	11/23/2021	11/23/2021
PREXPPOL			EMPL	020211204154398		$2,040.00			12/7/2021	12/7/2021	12/7/2021
PREXPPOL			EMPL	020211218141808		$1,935.00			12/21/2021	12/21/2021	12/21/2021
PREXPPOL			EMPL	020220101155948		$1,035.00			1/4/2022	1/4/2022	1/4/2022
PREXPPOL			EMPL	020220115135688		$2,055.00			1/18/2022	1/18/2022	1/18/2022
PREXPPOL			EMPL	020220129149508		$2,595.00			2/1/2022	2/1/2022	2/1/2022
PREXPPOL			EMPL	020220212156038		$1,920.00			2/15/2022	2/15/2022	2/15/2022
PREXPPOL			EMPL	020220226134278		$1,260.00			3/1/2022	3/1/2022	3/1/2022
PREXPPOL			EMPL	020220312135738		$2,250.00			3/15/2022	3/15/2022	3/15/2022
PREXPPOL			EMPL	020220326137338		$3,000.00			3/29/2022	3/29/2022	3/29/2022
PREXPPOL			EMPL	020220409137648		$2,820.00			4/12/2022	4/12/2022	4/12/2022
PREXPPOL			EMPL	020220423149038		$2,325.00			4/26/2022	4/26/2022	4/26/2022
PREXPPOL			EMPL	020220507136008		$1,905.00			5/10/2022	5/10/2022	5/10/2022
PREXPPOL			EMPL	020220521150458		$2,130.00			5/24/2022	5/24/2022	5/24/2022
PREXPPOL			EMPL	020220604123828		$480.00			6/7/2022	6/7/2022	6/7/2022
Summary for 'Object' = A01 (23 detail records)						*$48,570.00*					
Summary for 'Object_Class' = AA (23 detail records)						*$48,570.00*					
object_class	BB									
B01	Other Out Of State Travel - INCLUSIVE: AIRFARE, HOTEL, LODGI									
PREXPPOL			EMPL	020211009159058		$1,974.46			10/12/2021	10/12/2021	10/12/2021
PREXPPOL			EMPL	020211204154378		$689.40			12/7/2021	12/7/2021	12/7/2021
PREXPPOL			EMPL	020220226134268		$1,598.08			3/1/2022	3/1/2022	3/1/2022
Summary for 'Object' = B01 (3 detail records)						*$4,261.94*					
B02	In-State Travel									
PREXPPOL			EMPL	020220226134268		$175.21			3/1/2022	3/1/2022	3/1/2022
PREXPPOL			EMPL	020220702103958		$55.57			7/6/2022	7/6/2022	7/6/2022
Summary for 'Object' = B02 (2 detail records)						*$230.78*					
B05	Conference, Training, Registration and Membership Dues and L									
PREXPPOL			EMPL	020211009159058		$550.00			10/12/2021	10/12/2021	10/12/2021
PREXPPOL			EMPL	020211204154378		$150.00			12/7/2021	12/7/2021	12/7/2021
PREXPPOL			EMPL	020220226134268		$550.00			3/1/2022	3/1/2022	3/1/2022
PREXPPOL			EMPL	020220326137328		$154.00			3/29/2022	3/29/2022	3/29/2022
Summary for 'Object' = B05 (4 detail records)						*$1,404.00*					
Summary for 'Object_Class' = BB (9 detail records)						*$5,896.72*					
object_class	CC									
C23	Management, Business Professionals & Admin Services									
PREXPPOL			CNTR	020210731105478		$3,000.00			8/3/2021	8/3/2021	8/3/2021
PREXPPOL			CNTR	020210814103948		$3,000.00			8/17/2021	8/17/2021	8/17/2021

Appropriation	Program	BFY	Doc_ID_Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt		Accpt_Dt
PREXP	POL		CNTR	020210828104868		$3,000.00			8/31/2021	8/31/2021	8/31/2021
PREXP	POL		CNTR	020210911103958		$3,000.00			9/14/2021	9/14/2021	9/14/2021
PRADJ	POL		09152100000000004356			$3,035.00			9/15/2021	9/15/2021	9/15/2021
PRADJ	POL		09152100000000004355			$580.00			9/15/2021	9/15/2021	9/15/2021
PREXP	POL		CNTR	020210925104818		$3,000.00			9/28/2021	9/28/2021	9/28/2021
PREXP	POL		CNTR	020211009107198		$3,000.00			10/12/2021	10/12/2021	10/12/2021
PREXP	POL		CNTR	020211023106928		$3,000.00			10/26/2021	10/26/2021	10/26/2021
PREXP	POL		CNTR	020211106106858		$3,000.00			11/9/2021	11/9/2021	11/9/2021
PREXP	POL		CNTR	020211120106908		$3,000.00			11/23/2021	11/23/2021	11/23/2021
PREXP	POL		CNTR	020211204107268		$3,000.00			12/7/2021	12/7/2021	12/7/2021
PREXP	POL		CNTR	020211218104668		$3,000.00			12/21/2021	12/21/2021	12/21/2021
PREXP	POL		CNTR	020220101104698		$3,000.00			1/4/2022	1/4/2022	1/4/2022
PREXP	POL		CNTR	020220115102868		$3,000.00			1/18/2022	1/18/2022	1/18/2022
PREXP	POL		CNTR	020220129106238		$3,000.00			2/1/2022	2/1/2022	2/1/2022
PREXP	POL		CNTR	020220212107738		$3,000.00			2/15/2022	2/15/2022	2/15/2022
PREXP	POL		CNTR	020220226102998		$3,000.00			3/1/2022	3/1/2022	3/1/2022
PREXP	POL		CNTR	020220312103008		$3,000.00			3/15/2022	3/15/2022	3/15/2022
PREXP	POL		CNTR	020220326103218		$3,000.00			3/29/2022	3/29/2022	3/29/2022
PREXP	POL		CNTR	020220409103208		$3,000.00			4/12/2022	4/12/2022	4/12/2022
PREXP	POL		CNTR	020220423106868		$3,000.00			4/26/2022	4/26/2022	4/26/2022
PREXP	POL		CNTR	020220507102968		$3,000.00			5/10/2022	5/10/2022	5/10/2022
PREXP	POL		CNTR	020220521106788		$3,000.00			5/24/2022	5/24/2022	5/24/2022
PREXP	POL		CNTR	020220604105068		$3,000.00			6/7/2022	6/7/2022	6/7/2022
PREXP	POL		CNTR	020220618107118		$3,000.00			6/21/2022	6/21/2022	6/21/2022
Summary for 'Object' = C23 (26 detail records)						*$75,615.00*					
C98	Reimb Travel/Other Expenses CC Special Contract/Employee										
PREXP	POL		CNTR	020211218104658		$7.59			12/21/2021	12/21/2021	12/21/2021
PREXP	POL		CNTR	020211218104668		$26.16			12/21/2021	12/21/2021	12/21/2021
Summary for 'Object' = C98 (2 detail records)						*$33.75*					
Summary for 'Object_Class' = CC (28 detail records)						*$75,648.75*					
object_class	DD										
D09	Fringe Benefit Cost Recoupment										
CA	CTR		FRGEFRNG	0911210000001792		$2,421.79					9/11/2021
CA	CTR		PTXEPYTX	0911210000007689		$177.30					9/11/2021
CA	CTR		PTXEPYTX	0911210000007408		$127.36					9/11/2021
CA	CTR		FRGEFRNG	1010210000002420		$1,359.80					10/10/2021
CA	CTR		PTXEPYTX	1010210000010036		$71.51					10/10/2021
CA	CTR		PTXEPYTX	1010210000010429		$189.42					10/10/2021
CA	CTR		FRGEFRNG	1107210000003062		$2,011.60					11/7/2021
CA	CTR		PTXEPYTX	1107210000012600		$105.79					11/7/2021
CA	CTR		PTXEPYTX	1107210000012898		$118.20					11/7/2021
CA	CTR		FRGEFRNG	1204210000003705		$2,005.98					12/4/2021
CA	CTR		PTXEPYTX	1204210000015329		$118.20					12/4/2021
CA	CTR		PTXEPYTX	1204210000015063		$105.49					12/4/2021
CA	CTR		FRGEFRNG	0115220000004349		$1,489.04					1/15/2022
CA	CTR		PTXEPYTX	0115220000018441		$118.20					1/15/2022
CA	CTR		PTXEPYTX	0115220000018007		$78.31					1/15/2022
CA	CTR		FRGEFRNG	0205220000004987		$1,157.51					2/5/2022
CA	CTR		PTXEPYTX	0205220000021134		$118.20					2/5/2022
CA	CTR		PTXEPYTX	0205220000020855		$60.87					2/5/2022
CA	CTR		FRGEFRNG	0305220000005627		$1,691.32					3/5/2022
CA	CTR		PTXEPYTX	0305220000023716		$118.20					3/5/2022
CA	CTR		PTXEPYTX	0305220000023426		$88.95					3/5/2022
CA	CTR		FRGEFRNG	0409220000006301		$2,438.65					4/9/2022
CA	CTR		PTXEPYTX	0409220000026405		$177.30					4/9/2022
CA	CTR		PTXEPYTX	0409220000026119		$128.25					4/9/2022
CA	CTR		FRGEFRNG	0507220000006969		$1,927.32					5/7/2022
CA	CTR		PTXEPYTX	0507220000028701		$101.36					5/7/2022

Appropriation_Program	BFY	Doc_ID_Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
CA CTR PTXEPYTX0507220000028979					$118.20				5/7/2022
CA CTR FRGEFRNG0611220000007635					$1,511.51				6/11/2022
CA CTR PTXEPYTX0611220000031524					$118.20				6/11/2022
CA CTR PTXEPYTX0611220000031281					$79.49				6/11/2022
CA CTR FRGEFRNG0709220000000330					$179.81				7/9/2022
CA CTR PTXEPYTX0709220000002214					$9.46				7/9/2022
CA CTR PTXEPYTX0709220000002583					$118.20				7/9/2022
Summary for 'Object' = D09 (33 detail records)					*$20,640.79*				
Summary for 'Object_Class' = DD (33 detail records)					*$20,640.79*				
object_class EE									
E16 Indirect Cost Recoupment									
CA CTR INDE INDC0911210000002832					$1,134.61				9/11/2021
CA CTR INDE INDC1010210000003717					$637.07				10/10/2021
CA CTR INDE INDC1107210000004605					$942.44				11/7/2021
CA CTR INDE INDC1204210000005527					$939.80				12/4/2021
CA CTR INDE INDC0115220000006558					$697.61				1/15/2022
CA CTR INDE INDC0205220000007471					$542.30				2/5/2022
CA CTR INDE INDC0305220000008434					$792.38				3/5/2022
CA CTR INDE INDC0409220000009381					$1,142.51				4/9/2022
CA CTR INDE INDC0507220000010368					$902.95				5/7/2022
CA CTR INDE INDC0611220000011310					$708.14				6/11/2022
CA CTR INDE INDC0709220000000980					$84.24				7/9/2022
Summary for 'Object' = E16 (11 detail records)					*$8,524.05*				
Summary for 'Object_Class' = EE (11 detail records)					*$8,524.05*				
object_class UU									
U03 Software & Information Technology Licenses (IT)									
PRC POL 7214 PVPOL721422146SHI732	VC6000227588	SHI INTERNATIONAL CORP	B15154290	5/2/2022	$22,880.00	$0.00	$22,880.00	5/9/2022	5/9/2022	5/27/2022
Summary for 'Object' = U03 (1 detail record)					*$22,880.00*	*$0.00*	*$22,880.00*			
U10 Information Tech (IT) Equipment Maintenance & Repair									
PRC POL 7214 PVPOL721422068SHI129	VC6000227588	SHI INTERNATIONAL CORP	B13716166	1/20/2022	$136.00	$0.00	$136.00	1/13/2022	6/30/2022	3/11/2022
Summary for 'Object' = U10 (1 detail record)					*$136.00*	*$0.00*	*$136.00*			
Summary for 'Object_Class' = UU (2 detail records)					*$23,016.00*	*$0.00*	*$23,016.00*			
Summary for 'budget_fiscal_year' = 2022 (106 detail records)					*$182,296.31*	*$0.00*	*$23,016.00*			
2023									
object_class KK									
K10 Law Enforcement & Security Equipment									
PRC POL 7214 PVPOL721423102BAIN01	VC0000506451	BAIN COR INC	4146	3/23/2023	$254,700.00	$5,094.00	$249,606.00	4/6/2023	4/6/2023	4/13/2023
Summary for 'Object' = K10 (1 detail record)					*$254,700.00*	*$5,094.00*	*$249,606.00*			
Summary for 'Object_Class' = KK (1 detail record)					*$254,700.00*	*$5,094.00*	*$249,606.00*			
object_class UU									
U07 Information Technology (IT) Equipment									
PRC POL 7214 PVPOL7214125BAYSTA01	VC0000500765	BAY STATE ALARM SECURITY INC	11342	4/5/2023	$151,959.89	$3,039.20	$148,920.69	5/3/2023	5/3/2023	5/8/2023
Summary for 'Object' = U07 (1 detail record)					*$151,959.89*	*$3,039.20*	*$148,920.69*			
U12 Information Tech (IT) cloud services									
PRC POL 7214 PVPOL721423INSIGH001	VC6000239916	INSIGHT PUBLIC SECTOR INC	1101037368	3/23/2023	$160,442.91	$0.00	$160,442.91	3/23/2023	3/23/2023	4/10/2023
Summary for 'Object' = U12 (1 detail record)					*$160,442.91*	*$0.00*	*$160,442.91*			
Summary for 'Object_Class' = UU (2 detail records)					*$312,402.80*	*$3,039.20*	*$309,363.60*			
Summary for 'budget_fiscal_year' = 2023 (3 detail records)					*$567,102.80*	*$8,133.20*	*$558,969.60*			
2024									
object_class UU									
U07 Information Technology (IT) Equipment									

Appropriation	Program	BFY	Doc_ID_Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
PRC	POL 7214	PVPOL721424201	CDWUXX	VC6000240027	CDW GOVERNMENT LLC	KP68362 7/18/2023	$663.78	$3.32	$660.46	7/11/2023 7/11/2023	7/24/2023
PRC	POL 7214	PVPOL721424241	BSASIX	VC0000500765	BAY STATE ALARM SECURITY INC	11500 8/3/2023	$5,030.18	$0.00	$5,030.18	8/1/2023 8/1/2023	8/31/2023
Summary for 'Object' = U07 (2 detail records)							*$5,693.96*	*$3.32*	*$5,690.64*		
Summary for 'Object_Class' = UU (2 detail records)							*$5,693.96*	*$3.32*	*$5,690.64*		
Summary for 'budget_fiscal_year' = 2024 (2 detail records)							*$5,693.96*	*$3.32*	*$5,690.64*		
Summary for 'Program' = FSHSP20CFC (111 detail records)							*$755,093.07*	*$8,136.52*	*$587,676.24*		
Summary for 'Appropriation' = 80004692 (111 detail records)							*$755,093.07*	*$8,136.52*	*$587,676.24*		
Summary for 'Department' = POL (111 detail records)							*$755,093.07*	*$8,136.52*	*$587,676.24*		

Discount -$8,136.52
= $746,956.55 ✓

Appropriation_Program	BFY	Doc_ID_Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
2546									
Grand Total					*$755,093.07*	*$8,136.52*	*$587,676.24*		

Form Name: 2547
Submission Time: HLS Quarterly Report
October 13, 2023 10:03 am
Browser: Chrome 117.0.0.0 / Windows
IP Address: 170.63.192.1
Unique ID: 1151975349
Location:

Which subrecipient are you reporting data for in this quarterly progress report?	Other Agency
Please select which other agency you are reporting data for in this quarterly report.	MSP Commonwealth Fusion Center (CFC)

Reporting Information

Project Name	FSHSP20CFC
Federal Fiscal Year (FFY) Funding	FFY 2020

Contact Information

Reported by	Amy Thibault
Job Title	Intelligence Services Manager
Email Address	amy.thibault@pol.state.ma.us
Phone Number	(978) 451-3717

Reporting Period

Quarter Number	3
Reporting Period (Months)	July 1st - September 30th
Reporting Period (Year)	2023

Instructions

I. Planning

II. Organization

Regional Specialty Response Teams

III. Equipment

Equipment State Share Text	Additional equipment (brackets, cables and mounting hardware) for LPRs was received and put into use.

IV. Training

Exercise Program

Type of exercise	Seminar

V. Management and Administration

VI. Other Activities

VII. Challenges/Delays

VIII. Success Stories

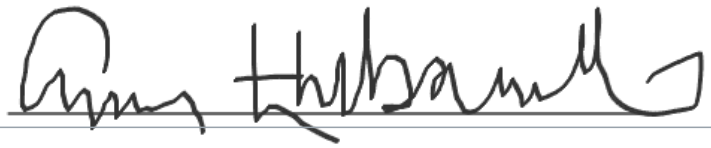
IX. Meetings

Waste, Fraud, or Abuse

Are you aware of any concerns regarding waste, fraud, or abuse connected to any of the grant-funded activities described in this report?	No

Fiduciary Coordinator Signature

Electronic Signature



Date	Oct 13, 2023

Submitting Your QR

2549

Reimbursable Grants Level 2

Menu

	Department	Major Program	Program	Funding Profile	Funding Priority	Funding Line	Obligation Ceiling	Pre Encumbered	Encumbered	Total Expenses
✓	POL	HSG2	FSHSP22CFC	FEDGRT	1	1	$375 000 00	$0 00	$4 485 00	$65 883 68

First Prev Next Last

Search

E pense Actuals

Pre Encumbered	$0.00	Obligation Ceiling	$375 000 00
Encumbered	$4 485 00	E penditure Ceiling	$375 000 00
Advances	$0.00	Uncommitted	$304 631 32
Accrued Expenses	$0 00	Une pended	$309 116 32
Cash E penses	$65,883 68	Back End plits	$0.00
Total Expenses	$65,883 68		
Charges	$0 00		

Revenue Actuals

Unbilled Earned Revenue	$0 00	Collected Earned Revenue	$55 711 18
Billed Earned Revenue	$10,172.50	Collected Unearned/De erred Revenue	$0 00
		Total Revenue	$65,883 68
		Revenue Credits	$0 00

Budgetary Amounts

Beginning Balance	$0 00	Revenue Beginning Balance	$0 00
Awarded	$375,000.00	Original Revenue Budget	$0 00
Amendments	$0 00	Revenue Amendments	$0 00
Trans er Out	$0.00	Current Revenue Budget	$0 00
Transfer In	$0 00	Unrecognized Revenue	($65 883 68)
Current Modi ied Budget	$375 000 00	Revenue Balance Forward	$0 00
Balance Forward	$0.00		

General In ormation

Department	POL	Name	FFY22 SHSP
Major Program	HSG2	tart Date	01/11/2023
Program	FSHSP22CFC	End Date	
Funding Pro ile	FEDGRT	Parent Dept	105
Funding Priority	1		EXECUTIVE OFFICE OF PUBLIC SAFETY & HOMELAND SECURITY
Funding Line	1	Description	
		Legal Cite	
		Active	☑

Top

Modified Budget Line Controls Previous Level

Grant Program Spending Report

Appropriation	Program	BFY	Doc_ID_Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
Dept: POL										
80004692	HOMELAND SECURITY II									
FSHSP22CFC	COMM FUSION CENTER									
		2023								
object_class	AA									
A01	Salaries: Inclusive									
PREXP	POL		EMPL 020230617152528			$2,768.00			6/20/2023	6/20/2023	6/20/2023
PREXP	POL		EMPL 020230701131767			$2,656.00			7/4/2023	7/4/2023	7/4/2023
Summary for 'Object' = A01 (2 detail records)						*$5,424.00*					
Summary for 'Object_Class' = AA (2 detail records)						*$5,424.00*					
object_class	DD									
D09	Fringe Benefit Cost Recoupment									
CA	CTR		PTXOPYTX0708230000002074			$100.34					7/8/2023
CA	CTR		FRGOFRNG0708230000000339			$2,142.48					7/21/2023
Summary for 'Object' = D09 (2 detail records)						*$2,242.82*					
Summary for 'Object_Class' = DD (2 detail records)						*$2,242.82*					
object_class	EE									
E16	Indirect Cost Recoupment									
CA	CTR		INDOINDC0708230000000863			$1,067.99					7/8/2023
Summary for 'Object' = E16 (1 detail record)						*$1,067.99*					
Summary for 'Object_Class' = EE (1 detail record)						*$1,067.99*					
object_class	KK									
K10	Law Enforcement & Security Equipment									
PRC	POL	7214	PVPOL721423118BODYAR	VC0000766104	BODY ARMOR OUTLET LLC	SO18320-INV34471	4/18/2023	$9,600.00	$24.00	$9,576.00	4/18/2023	4/18/2023	4/28/2023
PRC	POL	7214	PVPOL721423173GUARD1	VC0000203029	GUARDIAN UNIFORM & SUPPLY LLC	840744	6/8/2023	$9,075.00	$45.38	$9,029.62	6/20/2023	6/20/2023	6/26/2023
Summary for 'Object' = K10 (2 detail records)								*$18,675.00*	*$69.38*	*$18,605.62*			
Summary for 'Object_Class' = KK (2 detail records)								*$18,675.00*	*$69.38*	*$18,605.62*			
Summary for 'budget_fiscal_year' = 2023 (7 detail records)								*$27,409.81*	*$69.38*	*$18,605.62*			
		2024											
object_class	AA									
A01	Salaries: Inclusive									
PREXP	POL		EMPL 020230715143108			$2,680.00			7/18/2023	7/18/2023	7/18/2023
PREXP	POL		EMPL 020230729144958			$3,348.75			8/1/2023	8/1/2023	8/1/2023
PREXP	POL		EMPL 020230812141288			$2,537.50			8/15/2023	8/15/2023	8/15/2023
PREXP	POL		EMPL 020230826144288			$2,502.50			8/29/2023	8/29/2023	8/29/2023
PREXP	POL		EMPL 020230909170988			$2,870.00			9/12/2023	9/12/2023	9/12/2023
PREXP	POL		EMPL 020230923145038			$2,887.50			9/26/2023	9/26/2023	9/26/2023
Summary for 'Object' = A01 (6 detail records)						*$16,826.25*					
Summary for 'Object_Class' = AA (6 detail records)						*$16,826.25*					
object_class	CC									
C23	Management, Business Professionals & Admin Services									
PREXP	POL		CNTR 020230826102158			$7,400.00			8/29/2023	8/29/2023	8/29/2023
PREXP	POL		CNTR 020230909105588			$7,032.00			9/12/2023	9/12/2023	9/12/2023
PREXP	POL		CNTR 020230923104198			$7,285.00			9/26/2023	9/26/2023	9/26/2023
Summary for 'Object' = C23 (3 detail records)						*$21,717.00*					
Summary for 'Object_Class' = CC (3 detail records)						*$21,717.00*					
Summary for 'budget_fiscal_year' = 2024 (9 detail records)						*$38,543.25*					

Appropriation_Program	BFY	Doc_ID_Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
Summary for 'Program' = FSHSP22CFC (16 detail records)					*$65,953.06*	*$69.38*	*$18,605.62*		
Summary for 'Appropriation' = 80004692 (16 detail records)					*$65,953.06*	*$69.38*	*$18,605.62*		
Summary for 'Department' = POL (16 detail records)					*$65,953.06*	*$69.38*	*$18,605.62*		

Appropriation_Program	BFY	Doc_ID_Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
2552									
Grand Total					*$65,953.06*	*$69.38*	*$18,605.62*		

2553

Reimbursable Grants Level 2

Menu

	Department	Major Program	Program	Funding Profile	Funding Priority	Funding Line	Obligation Ceiling	Pre Encumbered	Encumbered	Total Expenses
✓	POL	UASI2	FUASI22CFC	FEDGRT	1	1	$375 000 00	$0 00	$0 00	$565 18

First Prev Next Last

Search

E pense Actuals

Pre Encumbered	$0.00	Obligation Ceiling	$375 000 00
Encumbered	$0 00	E penditure Ceiling	$375 000 00
Advances	$0.00	Uncommitted	$374 434 82
Accrued Expenses	$0 00	Une pended	$374 434 82
Cash E penses	$565.18	Back End plits	$0.00
Total Expenses	$565.18		
Charges	$0 00		

Revenue Actuals

Unbilled Earned Revenue	$0 00	Collected Earned Revenue	$565 18
Billed Earned Revenue	$0.00	Collected Unearned/De erred Revenue	$0 00
		Total Revenue	$565.18
		Revenue Credits	$0 00

Budgetary Amounts

Beginning Balance	$0 00	Revenue Beginning Balance	$0 00
Awarded	$375,000.00	Original Revenue Budget	$0 00
Amendments	$0 00	Revenue Amendments	$0 00
Trans er Out	$0.00	Current Revenue Budget	$0 00
Transfer In	$0 00	Unrecognized Revenue	($565 18)
Current Modi ied Budget	$375 000 00	Revenue Balance Forward	$0 00
Balance Forward	$0.00		

General In ormation

Department	POL	Name	FFY22 UASI
Major Program	UASI2	tart Date	01/11/2023
Program	FUASI22CFC	End Date	
Funding Pro ile	FEDGRT	Parent Dept	105
Funding Priority	1		EXECUTIVE OFFICE OF PUBLIC SAFETY & HOMELAND SECURITY
Funding Line	1	Description	
		Legal Cite	
		Active	☑

Top

Modified Budget Line Controls Previous Level

Grant Program Spending Report

Appropriation	Program	BFY	Doc_ID_Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
Dept: **POL**										
80004794 Urban Areas Initiative Grant										
	FUASI22CFC COMM FUSION CENTER									
		2023								
	object_class BB									
	B05 Conference, Training, Registration and Membership Dues and L									
			PREXPPOL	EMPL 020230128156118		$154.00			1/31/2023	1/31/2023 1/31/2023
	Summary for 'Object' = B05 (1 detail record)					*$154.00*				
	Summary for 'Object_Class' = BB (1 detail record)					*$154.00*				
	Summary for 'budget_fiscal_year' = 2023 (1 detail record)					*$154.00*				
		2024								
	object_class BB									
	B02 In-State Travel									
			PREXPPOL	EMPL 020230826144668		$411.18			8/29/2023	8/29/2023 8/29/2023
	Summary for 'Object' = B02 (1 detail record)					*$411.18*				
	Summary for 'Object_Class' = BB (1 detail record)					*$411.18*				
	Summary for 'budget_fiscal_year' = 2024 (1 detail record)					*$411.18*				
Summary for 'Program' = FUASI22CFC (2 detail records)						*$565.18*	✓			
Summary for 'Appropriation' = 80004794 (2 detail records)						*$565.18*				
Summary for 'Department' = POL (2 detail records)						*$565.18*				

Appropriation_Program	BFY	Doc_ID_Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
2555									
Grand Total					*$565.18*				

Form Name: 2556
Submission Time: HLS Quarterly Report
October 13, 2023 10:59 am
Browser: Chrome 117.0.0.0 / Windows
IP Address: 170.63.192.1
Unique ID: 1151999761
Location:

Which subrecipient are you reporting data for in this quarterly progress report?	Other Agency
Please select which other agency you are reporting data for in this quarterly report.	MSP Commonwealth Fusion Center (CFC)

Reporting Information

Project Name	FSHSP22CFC_FUASI22CFC
Federal Fiscal Year (FFY) Funding	FFY 2022

Contact Information

Reported by	Amy Thibault
Job Title	Intelligence Services Manager
Email Address	amy.thibault@pol.state.ma.us
Phone Number	(978) 451-3717

Reporting Period

Quarter Number	3
Reporting Period (Months)	July 1st - September 30th
Reporting Period (Year)	2023

Instructions

I. Planning

II. Organization

Regional Specialty Response Teams

III. Equipment

IV. Training

Training Name	CrimeTracer Training
Which of the following best describes the topic of this training?	Other: Crimetracer Database Training
Total number of participants attending this training	334
	Multidisciplinary training? = No Related to ASHER/complex coordinated attacks? = No
Which of the following core capabilities does this training address?	Intelligence and Information Sharing
Total number of sessions related to training in this reporting period.	9
Training Session Date(s)	Jul 11, 2023
Training Session Date (2)	Jul 12, 2023
Training Session Date (3)	Jul 13, 2023
Training Session Date (4)	Aug 08, 2023
Training Session Date (5)	Aug 09, 2023
Training Session Date (6)	Aug 10, 2023
Training Session Date (7)	Sep 12, 2023
Training Session Date (8)	Sep 13, 2023
Training Session Date (9)	Sep 14, 2023
Add another training?	No

Exercise Program

Type of exercise	Seminar

V. Management and Administration

VI. Other Activities

VII. Challenges/Delays

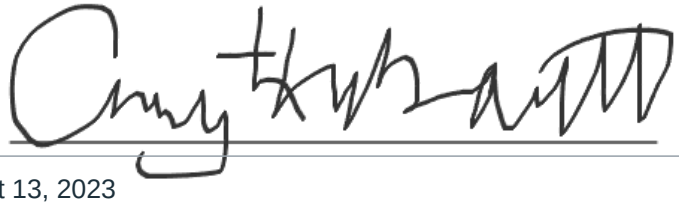
VIII. Success Stories

IX. Meetings

Waste, Fraud, or Abuse

Are you aware of any concerns regarding waste, fraud, or abuse connected to any of the grant-funded activities described in this report?	No

Fiduciary Coordinator Signature

Electronic Signature	
Date	Oct 13, 2023

Submitting Your QR

2559

Massachusetts Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Grant Division

QUARTERLY FINANCIAL REPORT

Agency/Contractor Name:	Massachusetts State Police	**Date:**	Tuesday, July 11, 2023
Project Name:	Continued Funding for the Critical Infrastructure Program	**E-mail:**	jeff.ly@pol.state.ma.us
Grant Program & FFY:	FUASI20CIP 8000-4794 FFY2020	**Telephone:**	508-988-7081
Reported by:	Jeff Ly	**FAX:**	508-820-2165

Report Number	Reporting Period	Year	Report Due
Quarter __	July 1st – September 30th	2022	October 15th
Quarter __	October 1st – December 31st	2022	January 15th
Quarter __	January 1st – March 31st	2023	April 15th
Quarter X	April 1st – June 30th	2023	July 15th

SUMMARY OF COSTS

Expense Category	Approved Budget	Expended This Quarter	Expended to Date	Obligated to Date	Balance	% Remaining
Salary	$0.00	$0.00	$0.00	$0.00	0.00	**0.00%**
Fringe	$0.00	$0.00	$0.00	$0.00	0.00	0.00%
Indirect	$0.00	$0.00	$0.00	$0.00	0.00	0.00%
Consultants/Contracts	$0.00	$0.00	$0.00	$0.00	0.00	0.00%
Travel	$335.00	$0.00	$335.00	$0.00	0.00	0.00%
Equipment	$78,547.93	$0.00	$0.00	$56,547.93	22,000.00	28.01%
Supplies	$2,062.51	$0.00	$0.00	$0.00	2,062.51	100.00%
Overtime	$0.00	$0.00	$0.00	$0.00	0.00	0.00%
Other (software, registrations, seminars)	$119,054.56	$0.00	$105,787.80	$0.00	13,266.76	11.14%
TOTAL	**$200,000.00**	**$0.00**	**$106,122.80**	**$56,547.93**	**$37,329.27**	18.66%

Reports must be submitted for every full or partial calendar quarter during the grant period regardless of spending activity.

Please send this report along with the Quarterly Financial Detail and Quarterly Progress Reports to:

Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720A
Boston, MA 02116
ATTN: Vicky Mboka-Boyer *via email*

Authorized Signature (Blue ink please)

Date

Kellie Gray

Print Name

Executive Office of Public Safety

Quarterly Financial Report (Detail for Expenditures)

Quarter Reporting Period (Choose From Cell Below) 4/1-6/30

Year Reporting Period (Choose From Cell Below) 2023

FFY20 FUASI20CIP

Salary:Please List all Employees charged to grant along with either: hours and rate, if paid hourly; or amount paid to employee for period from federal funds and a brief description, if salaried

Employee Name	Hrs/Unit	Rate/Amt	Description	Total	
				Sub-Total:	$0 00

Fringe: Fringe costs must go by Federally approved rate, and base amount should easily be identified from this detailed report.

Employee Name	Approved Rate	Base Amount			
				Sub-Total:	$0 00

Indirect: Indirect Rate must be a federally Negotiated and approved rate, and base amount should easily be identified from this detailed report.

Employee/Contracted Employee Name	Approved Rate	Base Amount		Total	
				Sub-Total:	$0.00

Consultants/Contracts: Please list Name of Consultant or Entity contract is with, hours and rate of contract and a brief description. If total costs for quarter for any single contract exceed $5K, please provide invoices for

Company/Name	Hours	Rate	Description	Total	
				Sub-Total:	$0 00

Travel: Please list each employee, cost of travel, description/purpose of travel, and the guidelines followed for reimbursement (Local, State, or Federal). Please include all receipts.

Employee Name	Cost	Guidelines	Purpose/Description	Total	Receipt Y/N
				Sub-Total:	$0 00

Piece of equipment	Unit Cost	Quantity	Description of Equipment	Total	Receipt
				Sub-Total:	$0 00

Supplies: Please list supplies and computation basis for reimbursement request.

Item	Cost		Basis for Computation	Total	
				Sub-Total:	$0 00

Overtime

Employee Name	Hrs/Unit	Rate/Amt	Description	Total	
				Sub-Total:	$0 00

Other: Please list Item and Basis for Computation.

Item	Cost	Qty	Basis for Computation	Total	Receipt
				$0.00	
				Sub-Total:	$0 00

Total

Total:* -

FUASI20CIP Travel FY'21	"T" Number if Applicable	DESCRIPTION	Dates of Travel	B01	B02	B05	B08	B10	C98 - Contracted	Total
Richard S. Range	T-21G-21	ASIS CPP Certification Conference, Training & Registration FEES				$ 335.00				$335.00
		TOTAL FOR 4/1/21 -06/30/2021							**$0.00**	$335.00

FUASI20CIP Travel FY'21	"T" Number if Applicable	DESCRIPTION	Dates of Travel	B01	B02	B05	B08	B10	C98 - Contracted	Total
										$0.00
										$0.00
										$0.00
										$0.00
										$0.00
										$0.00
										$0.00
										$0.00
		TOTAL FOR 7/1/21 - 9/30/21		**$0.00**	**$0.00**	**$0.00**	**$0.00**	**$0.00**	**$0.00**	**$0.00**

FSHSP18CCI TRAVEL FY 19	"T" Number if Applicable	DESCRIPTION	Dates of Travel	B01	B02	B05	B08	B10	C98 - Contracted	Total
		TOTAL FOR 10/1/17-12/31/17							**$0.00**	**$0.00**

2562

Reimbursable Grants: Level 2

Menu

	Department	Major Program	Program	Funding Profile	Funding Priority	Funding Line	Obligation Ceiling	Pre Encumbered	Encumbered	Total Expenses
✓	POL	UASI2	FUASI20CIP	FEDGRT	1	1	$200,000.00	$0.00	$56,547.93	$106,122.80

First Prev Next Last

Search

Expense Actuals

Pre Encumbered :	$0.00	Obligation Ceiling :	$200,000.00
Encumbered :	$56,547.93	Expenditure Ceiling :	$200,000.00
Advances :	$0.00	Uncommitted :	$37,329.27
Accrued Expenses :	$0.00	Unexpended :	$93,877.20
Cash Expenses :	$106,122.80	Back End Splits :	$0.00
Total Expenses :	$106,122.80		
Charges :	$0.00		

Revenue Actuals

Unbilled Earned Revenue :	$0.00	Collected Earned Revenue :	$106,122.80
Billed Earned Revenue :	$0.00	Collected Unearned/Deferred Revenue :	$0.00
		Total Revenue :	$106,122.80
		Revenue Credits :	$0.00

Budgetary Amounts

Beginning Balance :	$0.00	Revenue Beginning Balance :	$0.00
Awarded :	$200,000.00	Original Revenue Budget :	$0.00
Amendments :	$0.00	Revenue Amendments :	$0.00
Transfer Out :	$0.00	Current Revenue Budget :	$0.00
Transfer In :	$0.00	Unrecognized Revenue :	($106,122.80)
Current Modified Budget :	$200,000.00	Revenue Balance Forward :	$0.00
Balance Forward :	$0.00		

General Information

Department :	POL	Name :	FFY20 UASI
Major Program :	UASI2	Start Date :	12/15/2020
Program :	FUASI20CIP	End Date :	
Funding Profile :	FEDGRT	Parent Dept :	105
Funding Priority :	1	Description :	EXECUTIVE OFFICE OF PUBLIC SAFETY & HOMELAND SECURITY
Funding Line :	1	Legal Cite :	
		Active :	☑

Top

Modified Budget Line Controls Previous Level

Grant Program Spending Report

Appropriation	Program	BFY	Doc_ID	Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
Dept: POL											
80004794	Urban Areas Initiative Grant										
FUASI20CIP	CRITICAL INFRASTRUCTURE PROGRAM										
		2021									
object_class	BB										
B05	Conference, Training, Registration and Membership Dues and L										
PREXP	POL		EMPL 020210619143418				$335.00			6/22/2021	6/22/2021	6/22/2021
PRLNP	POL		EMPL 020210619143418				($335.00)			6/22/2021	6/22/2021	6/22/2021
PRLNP	POL		EMPL 020210619143418				$335.00			6/22/2021	6/22/2021	6/22/2021
Summary for 'Object' = B05 (3 detail records)							*$335.00*					
Summary for 'Object_Class' = BB (3 detail records)							*$335.00*					
object_class	UU										
U03	Software & Information Technology Licenses (IT)										
PRC	POL	7214	PVPOL721421022SHI646	VC6000227588	SHI INTERNATIONAL CORP	B12888177	1/19/2021	$3,387.70	$0.00	$3,387.70	1/15/2021	6/30/2021	1/22/2021
EFT	CTR		DISB0304210000283978	VC6000227588	SHI INTERNATIONAL CORP	B12888177	1/19/2021	($3,387.70)			1/15/2021	6/30/2021	3/4/2021
EFT	CTR		DISB0304210000283978	VC6000227588	SHI INTERNATIONAL CORP	B12888177	1/19/2021	$3,387.70			1/15/2021	6/30/2021	3/4/2021
PRC	POL	7214	PVPOL721421095SHI783	VC6000227588	SHI INTERNATIONAL CORP	B13256542	4/1/2021	$24,099.10	$0.00	$24,099.10	4/1/2021	6/30/2021	4/5/2021
EFT	CTR		DISB0513210000077772	VC6000227588	SHI INTERNATIONAL CORP	B13256542	4/1/2021	$24,099.10			4/1/2021	6/30/2021	5/13/2021
EFT	CTR		DISB0513210000077772	VC6000227588	SHI INTERNATIONAL CORP	B13256542	4/1/2021	($24,099.10)			4/1/2021	6/30/2021	5/13/2021
PRC	POL	7214	PVPOL721421137SHI867	VC6000227588	SHI INTERNATIONAL CORP	B13460708	5/14/2021	$3,179.00	$0.00	$3,179.00	5/17/2021	5/17/2021	5/17/2021
EFT	CTR		DISB0628210000262057	VC6000227588	SHI INTERNATIONAL CORP	B13460708	5/14/2021	($3,179.00)			5/17/2021	5/17/2021	6/28/2021
EFT	CTR		DISB0628210000262057	VC6000227588	SHI INTERNATIONAL CORP	B13460708	5/14/2021	$3,179.00			5/17/2021	5/17/2021	6/28/2021
Summary for 'Object' = U03 (9 detail records)							*$30,665.80*	*$0.00*	*$30,665.80*			
Summary for 'Object_Class' = UU (9 detail records)							*$30,665.80*	*$0.00*	*$30,665.80*			
Summary for 'budget_fiscal_year' = 2021 (12 detail records)							*$31,000.80*	*$0.00*	*$30,665.80*			
		2022										
object_class	EE										
EE2	Conference, Training and Registration Fees										
GAX	POL	7214	PVPOL721422697ESCAL1	VC6000249640	ESCAL INSTITUTE OF ADVANCED TEC	AGGREGATE-69950-101325	5/15/2021	$47,748.00	$0.00	$47,748.00	7/15/2021	7/15/2021	7/16/2021
AD	CTR		DISB0719210000532665	VC6000249640	ESCAL INSTITUTE OF ADVANCED TEC	AGGREGATE-69950-101325	5/15/2021	$47,748.00			7/15/2021	7/15/2021	7/19/2021
AD	CTR		DISB0719210000532665	VC6000249640	ESCAL INSTITUTE OF ADVANCED TEC	AGGREGATE-69950-101325	5/15/2021	($47,748.00)			7/15/2021	7/15/2021	7/19/2021
Summary for 'Object' = EE2 (3 detail records)							*$47,748.00*	*$0.00*	*$47,748.00*			
Summary for 'Object_Class' = EE (3 detail records)							*$47,748.00*	*$0.00*	*$47,748.00*			
object_class	UU										
U11	Information Technology (IT) Contract Services										
PRC	POL	7214	PVPOL721422174SHI754	VC6000227588	SHI INTERNATIONAL CORP	B15384250	6/21/2022	$27,374.00	$0.00	$27,374.00	5/16/2022	5/18/2022	6/24/2022
EFT	CTR		DISB0802220000112385	VC6000227588	SHI INTERNATIONAL CORP	B15384250	6/21/2022	($27,374.00)			5/16/2022	5/18/2022	8/2/2022
EFT	CTR		DISB0802220000112385	VC6000227588	SHI INTERNATIONAL CORP	B15384250	6/21/2022	$27,374.00			5/16/2022	5/18/2022	8/2/2022
Summary for 'Object' = U11 (3 detail records)							*$27,374.00*	*$0.00*	*$27,374.00*			
Summary for 'Object_Class' = UU (3 detail records)							*$27,374.00*	*$0.00*	*$27,374.00*			
Summary for 'budget_fiscal_year' = 2022 (6 detail records)							*$75,122.00*	*$0.00*	*$75,122.00*			
Summary for 'Program' = FUASI20CIP (18 detail records)							*$106,122.80*	*$0.00*	*$105,787.80*			
Summary for 'Appropriation' = 80004794 (18 detail records)							*$106,122.80*	*$0.00*	*$105,787.80*			
Summary for 'Department' = POL (18 detail records)							*$106,122.80*	*$0.00*	*$105,787.80*			

Appropriation_Program	BFY	Doc_ID_Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
2564									
Grand Total					*$106,122.80*	*$0.00*	*$105,787.80*		

2565

Massachusetts Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Grant Division

QUARTERLY FINANCIAL REPORT

Agency/Contractor Name:	Massachusetts State Police	**Date:**	Thursday, October 5, 2023
Project Name:	Continued Funding for the Critical Infrastructure Program	**E-mail:**	jeff.ly@pol.state.ma.us
Grant Program & FFY:	FUASI20CIP 8000-4794 FFY2020	**Telephone:**	508-988-7081
Reported by:	Jeff Ly	**FAX:**	508-820-2165

Report Number	Reporting Period	Year	Report Due
Quarter _X_	July 1st – September 30th	2023	October 15th
Quarter __	October 1st – December 31st	2023	January 15th
Quarter __	January 1st – March 31st	2024	April 15th
Quarter __	April 1st – June 30th	2024	July 15th

SUMMARY OF COSTS

Expense Category	Approved Budget	Expended This Quarter	Expended to Date	Obligated to Date	Balance	% Remaining
Salary	$0.00	$0.00	$0.00	$0.00	0.00	**0.00%**
Fringe	$0.00	$0.00	$0.00	$0.00	0.00	0.00%
Indirect	$0.00	$0.00	$0.00	$0.00	0.00	0.00%
Consultants/Contracts	$0.00	$0.00	$0.00	$0.00	0.00	0.00%
Travel	$335.00	$0.00	$335.00	$0.00	0.00	0.00%
Equipment	$78,547.93	$56,547.93	$56,547.93	$0.00	22,000.00	28.01%
Supplies	$2,062.51	$0.00	$0.00	$0.00	2,062.51	100.00%
Overtime	$0.00	$0.00	$0.00	$0.00	0.00	0.00%
Other (software, registrations, seminars)	$119,054.56	$0.00	$105,787.80	$13,266.76	0.00	0.00%
TOTAL	**$200,000.00**	**$56,547.93**	**$162,670.73**	**$13,266.76**	**$24,062.51**	12.03%

Reports must be submitted for every full or partial calendar quarter during the grant period regardless of spending activity.

Please send this report along with the Quarterly Financial Detail and Quarterly Progress Reports to:

Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720A
Boston, MA 02116
ATTN: Vicky Mboka-Boyer *via email*

R. Rust
Authorized Signature (Blue ink please)

10/11/23
Date

Rebecca Rust
Print Name

Executive Office of Public Safety

Quarterly Financial Report (Detail for Expenditures)

Quarter Reporting Period (Choose From Cell Below) 7/1-9/30

Year Reporting Period (Choose From Cell Below) 2023

FFY20 FUASI20CIP

Salary:Please List all Employees charged to grant along with either: hours and rate, if paid hourly; or amount paid to employee for period from federal funds and a brief description, if salaried

Employee Name	Hrs/Unit	Rate/Amt	Description	Total	
				Sub-Total:	$0.00

Fringe: Fringe costs must go by Federally approved rate, and base amount should easily be identified from this detailed report.

Employee Name	Approved Rate	Base Amount			
				Sub-Total:	$0.00

Indirect: Indirect Rate must be a federally Negotiated and approved rate, and base amount should easily be identified from this detailed report.

Employee/Contracted Employee Name	Approved Rate	Base Amount		Total	
				Sub-Total:	$0.00

Consultants/Contracts: Please list Name of Consultant or Entity contract is with, hours and rate of contract and a brief description. If total costs for quarter for any single contract exceed $5K, please provide invoices for

Company/Name	Hours	Rate	Description	Total	
				Sub-Total:	$0.00

Travel: Please list each employee, cost of travel, description/purpose of travel, and the guidelines followed for reimbursement (Local, State, or Federal). Please include all receipts.

Employee Name	Cost	Guidelines	Purpose/Description	Total	Receipt Y/N
				Sub-Total:	$0.00

Piece of equipment	Unit Cost	Quantity	Description of Equipment	Total	Receipt
BSA - Mobile Video Converter Kit	$ 56,547.93	1.00	Mobile video converter kit	$56,547.93	$ 56,547.93
				Sub-Total:	$56,547.93

Supplies: Please list supplies and computation basis for reimbursement request.

Item	Cost		Basis for Computation	Total	
				Sub-Total:	$0.00

Overtime

Employee Name	Hrs/Unit	Rate/Amt	Description	Total	
				Sub-Total:	$0.00

Other: Please list Item and Basis for Computation.

Item	Cost	Qty	Basis for Computation	Total	Receipt
				$0.00	
				Sub-Total:	$0.00

Total

Total:*	56,547.93

2567

Reimbursable Grants Level 2

Menu

Department	Major Program	Program	Funding Profile	Funding Priority	Funding Line	Obligation Ceiling	Pre Encumbered	Encumbered	Total Expenses
POL	UASI2	FUASI20C P	FEDGRT	1	1	$200 000 00	$0 00	$0 00	$175 937 49

First Prev Next Last

Search

E pense Actuals

Pre Encumbered	$0.00	Obligation Ceiling	$200 000 00
Encumbered	$0 00	E penditure Ceiling	$200 000 00
Advances	$0.00	Uncommitted	$24 062 51
Accrued Expenses	$13 266 76	Une pended	$24 062 51
Cash E penses	$162,670.73	Back End plits	$0.00
Total Expenses	$175,937.49		
Charges	$0 00		

Revenue Actuals

Unbilled Earned Revenue	$0 00	Collected Earned Revenue	$162 670 73
Billed Earned Revenue	$0.00	Collected Unearned/De erred Revenue	$0 00
		Total Revenue	$162,670.73
		Revenue Credits	$0 00

Budgetary Amounts

Beginning Balance	$0 00	Revenue Beginning Balance	$0 00
Awarded	$200,000.00	Original Revenue Budget	$0 00
Amendments	$0 00	Revenue Amendments	$0 00
Transfer Out	$0.00	Current Revenue Budget	$0 00
Transfer In	$0 00	Unrecognized Revenue	($162 670 73)
Current Modi ied Budget	$200 000 00	Revenue Balance Forward	$0 00
Balance Forward	$0.00		

General In ormation

Department	POL	Name	FFY20 UASI
Major Program	UASI2	tart Date	12/15/2020
Program	FUASI20C P	End Date	
Funding Pro ile	FEDGRT	Parent Dept	105
Funding Priority	1	Description	EXECUTIVE OFFICE OF PUBLIC SAFETY & HOMELAND SECURITY
Funding Line	1		
		Legal Cite	
		Active	☑

Top

Modified Budget Line Controls Previous Level

FUASI20CIP
8000-4794

fiscal year	department	doc code	cash_expense amount	service_from date	service_to date	appropriation	object	object_name	vendor_customer code	legal name	program	acceptance date
2021	POL	EFT	$ 3,387.70	15-Jan-21	30-Jun-21	80004794	U03	Software & Information Technology Licen	VC6000227588	SHI INTERNATIC	FUASI20CIP	04-Mar-21
2021	POL	EFT	$ 24,099.10	01-Apr-21	30-Jun-21	80004794	U03	Software & Information Technology Licen	VC6000227588	SHI INTERNATIC	FUASI20CIP	13-May-21
2021	POL	EFT	$ 3,179.00	17-May-21	17-May-21	80004794	U03	Software & Information Technology Licen	VC6000227588	SHI INTERNATIC	FUASI20CIP	28-Jun-21
2021	POL	PRLNP	$ 335.00	22-Jun-21	22-Jun-21	80004794	B05	Conference, Training, Registration and M			FUASI20CIP	22-Jun-21
2022	POL	AD	$ 47,748.00	15-Jul-21	15-Jul-21	80004794	EE2	Conference, Training and Registration Fe	VC6000249640	ESCAL INSTITUT	FUASI20CIP	19-Jul-21
2023	POL	EFT	$ 27,374.00	16-May-22	18-May-22	80004794	U11	Information Technology (IT) Contract Serv	VC6000227588	SHI INTERNATIC	FUASI20CIP	02-Aug-22
2024	POL	EFT	$ 56,547.93	13-Jul-23	13-Jul-23	80004794	U07	Information Technology (IT) Equipment	VC0000500765	BAY STATE ALA	FUASI20CIP	25-Aug-23

Total ALL Expenditures to 9/30/2023	162,670.73

View All 1 of 6 | Document validated successfully

Pymt Request-CommodityBased(PRC) Dept: POL ID: PVPOL721424223BSAXXX Ver.: 1 Function: New Phase: Draft

Final 8/11/23

Document Navigator 1/2023

Vendor Total Lines: 1 Vendor Line: 1 Vendor Customer: VC0000500765 Legal Name: BAY STATE ALARM SECURITY INC

	Vendor Line	Vendor Customer	Legal Name	Line Amount		
	1	VC0000500765	BAY STATE ALARM SECURITY INC	56547.93		

From 1 to 1 Total: 1

FUASI2301P Unit # 7214 8000-4794

General Information

Vendor Customer: VC0000500765
Legal Name: BAY STATE ALARM SECUR
Alias/DBA: BSA SECURITY INTEGRAT
Address Code: AD001
Address 1: 462 PLEASANT ST
Address 2:
City: MARLBOROUGH
State: Massachusetts
Zip Code: 01752-1127
Country: USA
County:

Vendor Contact ID:
Vendor Contact Name: Cindy McStay
Vendor Contact Phone: 508-485-1174
Vendor Contact Phone Ext.: 112
Vendor Contact Email: cindy@bsasi.com
Fax:
Fax Extension:
Web Address http://:
Taxpayer ID Number:
Taxpayer ID Type:
Merchant ID:
Tax Profile:
Received Service From Date:
Received Service To Date:

Disbursement Options

Disbursement Type: EFT
Disbursement Format: CTX
Scheduled Payment Date: 08/25/2023
Disbursement Priority: 99
Single Payment: ☐
Pay Third Party: ☐
On-line Disbursement Rqst: ☐
EFT Status: Eligible for EFT

Handling Code:
Disbursement Category: 100

Invoice Information

Invoice Doc Code:
Invoice Doc Dept:
Invoice Doc ID:

Vendor Invoice Number:
Vendor Invoice Date:
Tracking Date:

FUASI20CIP
Unit # 7214
8055-4794

Security Integrators

GSA Advantage!

INVOICE

Invoice Number: 11472
Invoice Date: Jul 14, 2023
Page: 1

Bay State Alarm Security, Inc.
462 Pleasant Street, Marlboro, MA 01752
Phone 508-485-1174 Fax 508-624-6568

Bill To:
Massachusetts State Police General 470 Worcester Road Framingham, MA 01702

Job:
2023BSASIU07POL20695 Mobile Video Converter Kit

Customer ID	Customer PO	Payment Terms	
MA State Police	2023BSASIU07POL20695	Net 30 Days	
Service Tech ID	Job Ticket ID	Date of Service	Due Date
		7/10/23	8/13/23

Quantity	Item	Description	Unit Price	Amount
[redacted] G.L. c. 4,sec. 7	a	Mobile Video Converter Kit	[redacted] G.L. c. 4,sec. 7, cl.24	56,547.93

Invoice Receipt date 7/14/23

"The equipment, goods or services for which this payment is made were received on 7/13/23"

certified by [signature]

signature date 7/20/23

Subtotal	56,547.93
Sales Tax	
Total Invoice Amount	56,547.93
Payment/Credit Applied	
TOTAL	56,547.93

Check/Credit Memo No:

GSA Advantage!

SDVOSB

BSA Security Integrators

SDVOSB

Packing Slip

MSP033023.1

Bay State Alarm Security, Inc. * 482 Pleasant Street * Marlboro, MA 01752 Ph 508-485-1174 Fax 508-624-6068

To: Massachusetts State Police
Division of Homeland Security
470 Worcester Road
Framingham, MA 01702

From: James P McStay Sr

Re: Mobile Video Converter Kit

Date: 7/13/23

Facility: Massachusetts State Police
Contact: Sgt. James Deas

Job: Provision of Mobile Video Converter Kit

#	U/M	DESCRIPTION		
1	Ea	20 SPACE 20U 24" DEEP HEAVY DUTY 3/8" PLY ATA RACK CASE		
2	Ea	FORTINET FIREWALL APPLIANCE ONLY – NO SOFTWARE/ UTM		
3	Ea	NETGEAR 48-PORT NETWORK SWITCH		
4	Ea	BLACK MAGIC DESIGN 6DI TO HDMI 6G CONVERTER		
5	Ea	CONNECTRONICS RACK MOUNT (10 SDI CONVERTERS 3U)		
6	Ea	BLACK MAGIC POWER UNITS		
7	Ea	BARCO ENCODER/DECODER (COMPACT DUAL CHANNEL 4K)		
8	Ea	BARCO RACK MOUNT (1U FOR 2 ENCODERS)		
9	Ea	TRIPPLITE 2400W 120V 3U RACK-MOUNT POWER CONDITIONER		
10	Ea	TRIPPLITE P569-003		
11	Ea	BELKIN 6' CAT6 550MHz GIGABIT SNAGLESS PATCH CABLES		
12	Ea	BELKIN 1' CAT6 550MHz GIGABIT SNAGLESS PATCH CABLES		

Received July 13, 2023
Sgt. [redacted] # 2337
James Deas

Grant Program Spending Report

Appropriation	Program	BFY	Doc_ID_Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
Dept: POL										
80004794	Urban Areas Initiative Grant									
FUASI20CIP	CRITICAL INFRASTRUCTURE PROGRAM									
		2021								
object_class	BB									
B05	Conference, Training, Registration and Membership Dues and L									
PREXP	POL		EMPL 020210619143418			$335.00			6/22/2021	6/22/2021	6/22/2021
Summary for 'Object' = B05 (1 detail record)						*$335.00*				
Summary for 'Object_Class' = BB (1 detail record)						*$335.00*				
object_class	UU									
U03	Software & Information Technology Licenses (IT)									
PRC	POL	7214	PVPOL721421022SHI646	VC6000227588	SHI INTERNATIONAL CORP	B12888177	1/19/2021	$3,387.70	$0.00	$3,387.70	1/15/2021	6/30/2021	1/22/2021
PRC	POL	7214	PVPOL721421095SHI783	VC6000227588	SHI INTERNATIONAL CORP	B13256542	4/1/2021	$24,099.10	$0.00	$24,099.10	4/1/2021	6/30/2021	4/5/2021
PRC	POL	7214	PVPOL721421137SHI867	VC6000227588	SHI INTERNATIONAL CORP	B13460708	5/14/2021	$3,179.00	$0.00	$3,179.00	5/17/2021	5/17/2021	5/17/2021
Summary for 'Object' = U03 (3 detail records)								*$30,665.80*	*$0.00*	*$30,665.80*			
Summary for 'Object_Class' = UU (3 detail records)								*$30,665.80*	*$0.00*	*$30,665.80*			
Summary for 'budget_fiscal_year' = 2021 (4 detail records)								*$31,000.80*	*$0.00*	*$30,665.80*			
		2022								
object_class	EE									
EE2	Conference, Training and Registration Fees									
GAX	POL	7214	PVPOL721422697ESCAL1	VC6000249640	ESCAL INSTITUTE OF ADVANCED TECAGGREGATE-69950-101325		7/15/2021	$47,748.00	$0.00	$47,748.00	7/15/2021	7/15/2021	7/16/2021
Summary for 'Object' = EE2 (1 detail record)								*$47,748.00*	*$0.00*	*$47,748.00*			
Summary for 'Object_Class' = EE (1 detail record)								*$47,748.00*	*$0.00*	*$47,748.00*			
object_class	UU									
U11	Information Technology (IT) Contract Services									
PRC	POL	7214	PVPOL721422174SHI754	VC6000227588	SHI INTERNATIONAL CORP	B15384250	6/21/2022	$27,374.00	$0.00	$27,374.00	5/16/2022	5/18/2022	6/24/2022
Summary for 'Object' = U11 (1 detail record)								*$27,374.00*	*$0.00*	*$27,374.00*			
Summary for 'Object_Class' = UU (1 detail record)								*$27,374.00*	*$0.00*	*$27,374.00*			
Summary for 'budget_fiscal_year' = 2022 (2 detail records)								*$75,122.00*	*$0.00*	*$75,122.00*			
		2024								
object_class	UU									
U03	Software & Information Technology Licenses (IT)									
PRC	POL	7214	PVPOL721424263SHICOX	VC6000227588	SHI INTERNATIONAL CORP	B17258818	9/5/2023	$13,266.76	A			1/28/2023	1/28/2024	9/20/2023
Summary for 'Object' = U03 (1 detail record)								*$13,266.76*						
U07	Information Technology (IT) Equipment									
PRC	POL	7214	PVPOL721424223BSAXXX	VC0000500765	BAY STATE ALARM SECURITY INC	11472	7/14/2023	$56,547.93	$0.00	$56,547.93	7/13/2023	7/13/2023	8/11/2023
Summary for 'Object' = U07 (1 detail record)								*$56,547.93*	*$0.00*	*$56,547.93*			
Summary for 'Object_Class' = UU (2 detail records)								*$69,814.69*	*$0.00*	*$56,547.93*			
Summary for 'budget_fiscal_year' = 2024 (2 detail records)								*$69,814.69*	*$0.00*	*$56,547.93*			
Summary for 'Program' = FUASI20CIP (8 detail records)								*$175,937.49*	*$0.00*	*$162,335.73*			
Summary for 'Appropriation' = 80004794 (8 detail records)								*$175,937.49*	*$0.00*	*$162,335.73*			
Summary for 'Department' = POL (8 detail records)								*$175,937.49*	*$0.00*	*$162,335.73*			

Appropriation_Program	BFY	Doc_ID_Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
2575									
Grand Total					*$175,937.49*	*$0.00*	*$162,335.73*		

A - $13,266.76 Accrued Exp
= $162,670.73

Form Name: 2574
Submission Time: HLS Quarterly Report
October 13, 2023 11:14 am
Browser: Chrome 117.0.0.0 / Windows
IP Address: 170.63.192.1
Unique ID: 1152005914
Location:

Which subrecipient are you reporting data for in this quarterly progress report?	Other Agency
Please select which other agency you are reporting data for in this quarterly report.	MSP Commonwealth Fusion Center (CFC)

Reporting Information

Project Name	FUSAI20CIP
Federal Fiscal Year (FFY) Funding	FFY 2020

Contact Information

Reported by	Amy Thibault
Job Title	Intelligence Services Manager
Email Address	amy.thibault@pol.state.ma.us
Phone Number	(978) 451-3717

Reporting Period

Quarter Number	3
Reporting Period (Months)	July 1st - September 30th
Reporting Period (Year)	2023

Instructions

I. Planning

II. Organization

Regional Specialty Response Teams

III. Equipment

IV. Training

Exercise Program

Type of exercise	Seminar

V. Management and Administration

VI. Other Activities

Other Activities State Share Text	We have held demos for the Smart Board that is to be purchased with this grant and are finalizing specifications.

VII. Challenges/Delays

VIII. Success Stories

IX. Meetings

Waste, Fraud, or Abuse

Are you aware of any concerns regarding waste, fraud, or abuse connected to any of the grant-funded activities described in this report?	No

Fiduciary Coordinator Signature

Electronic Signature



Date	Oct 13, 2023

Submitting Your QR

2576

Massachusetts Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Grant Division

QUARTERLY FINANCIAL REPORT

Agency/Contractor Name:	Massachusetts State Police	**Date:**	Friday, October 6, 2023
Project Name:	Continued Funding for the Critical Infrastructure Program	**E-mail:**	jeff.ly@pol.state.ma.us
Grant Program & FFY:	FUASI21COM 8000-4794	**Telephone:**	508-988-7081
Reported by:	Jeff Ly	**FAX:**	508-820-2165

Report Number	Reporting Period	Year	Report Due
Quarter _X__	July 1st – September 30th	2023	October 15th
Quarter ___	October 1st – December 31st	2023	January 15th
Quarter ___	January 1st – March 31st	2024	April 15th
Quarter ___	April 1st – June 30th	2024	July 15th

SUMMARY OF COSTS

Expense Category	Approved Budget	Expended This Quarter	Expended to Date	Obligated to Date	Balance	% Remaining
Salary	$0.00	$0.00	$0.00	$0.00	$0.00	0%
Fringe	$1,539.20	$178.63	$1,451.39	$0.00	$87.81	6%
Indirect	$0.00	$0.00	$0.00	$0.00	$0.00	0%
Consultants/Contracts	$83,200.00	$12,871.00	$88,085.50	$0.00	($4,885.50)	-6%
Travel	$20,000.00	$45.55	$595.17	$0.00	$19,404.83	97%
Equipment	$0.00	$0.00	$0.00	$0.00	$0.00	0%
Supplies	$3,858.96	$0.00	$0.00	$0.00	$3,858.96	100%
Overtime	$0.00	$0.00	$0.00	$0.00	$0.00	0%
Other (software, registrations, seminars)	$91,401.84	$0.00	$66,025.33	$0.00	$25,376.51	28%
TOTAL	**$200,000.00**	**$13,095.18**	**$156,157.39**	**$0.00**	**$43,842.61**	22%

Reports must be submitted for every full or partial calendar quarter during the grant period regardless of spending activity.

Please send this report along with the Quarterly Financial Detail and Quarterly Progress Reports to:

Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720A

Boston, MA 02116
ATTN: Vicky Mboka-Boyer *via email*

Rebecca Rust

Authorized Signature (Blue ink please)

10/11/2023

Date

Rebecca Rust

Print Name

*** NOTE: $9,632 was transferred out of consultants on 10/3/2023 and will be reflected on our next quarterly report. These charges should have been applied to FUASI22CIP.

Executive Office of Public Safety

Quarterly Financial Report (Detail for Expenditures)

Quarter Reporting Period (Choose From Cell Below) 7/1-9/30

Year Reporting Period (Choose From Cell Below) 2023

FFY 2020 FUASI21COM

Salary Please List all Employees charged to grant along with either: hours and rate, if paid hourly; or amount paid to employee for period from federal funds and a brief description, if salaried

Employee Name	Hrs/Unit	Rate/Amt	Description	Total	
				Sub-Total:	$0.00

Fringe: Fringe costs must go by Federally approved rate, and base amount should easily be identified from this detailed report.

Employee Name	Approved Rate	Base Amount			
Zayas, Joel	0 0185	$9,655 50	Payroll Tax for pay period end dates 6/3/23 - 7/1/23		$178 63
				Sub-Total:	$178.63

Indirect: Indirect Rate must be a federally Negotiated and approved rate, and base amount should easily be identified from this detailed report.

Employee/Contracted Employee Name	Approved Rate	Base Amount		Total	
				Sub-Total:	$0.00

Consultants/Contracts: Please list Name of Consultant or Entity contract is with, hours and rate of contract and a brief description. If total costs for quarter for any single contract exceed $5K, please provide invoices for

Company/Name	Hours	Rate	Description	Total	
Zayas, Joel	79.00	41 00	Payroll for pay period end date 04/08/23		3,239.00
Zayas, Joel	72.00	43 00	Payroll for pay period end date 04/22/23		3,096.00
Zayas, Joel	72.00	43 00	Payroll for pay period end date 05/06/22		3,096.00
Zayas, Joel	80.00	43 00	Payroll for pay period end date 05/20/23		3,440.00
					-
					-
					-
					-
				Sub-Total:	$12,871.00

Travel: Please list each employee, cost of travel, description/purpose of travel, and the guidelines followed for reimbursement (Local, State, or Federal). Please include all receipts.

Employee Name	Cost	Guidelines	Purpose/Description	Total	Receipt Y/N
Zayas, Joel	$ 45.55		Travel to Boston, MA for Amtrak/RAILSAFE training on May 16 - 17, 2022	$45.55	Y
				Sub-Total:	$45.55

Piece of equipment	Unit Cost	Quantity	Description of Equipment	Total	Receipt
				Sub-Total:	$0.00

Supplies: Please list supplies and computation basis for reimbursement request.

Item	Cost		Basis for Computation	Total	
				Sub-Total:	$0.00

Overtime

Employee Name	Hrs/Unit	Rate/Amt	Description	Total	
				Sub-Total:	$0.00

Other: Please list tem and Basis for Computation.

Item	Cost	Qty	Basis for Computation	Total	Receipt
				Sub-Total:	$0.00

Total

Total:*	$13,095.18

FUASI21COM TRAVEL EXPENSES

"T" Number if Appli		DESCRIPTION	Dates of Travel	B01	B02	B05	B08	B10	C98 - Contracted	Total
Dan Coleman	T-41G-22	National Cyber Crime Conference - Norwood MA	04/26/ -04/28	$ 118.17		$ 345.00				$463.17
Kaitlyn Duval	T-41G-22	National Cyber Crime Conference - Norwood MA	04/26/ -04/28	$ 73.36		$ 395.00				$468 36
Lindsey Nystrom	T-41G-22	National Cyber Crime Conference - Norwood MA	04/26/ -04/28		$ 80.48	$ 395.00				$475.48
Justin Salvatore	T-41G-22	National Cyber Crime Conference - Norwood MA	04/26/ -04/28	$ 73.46		$ 395.00				$468.46
Lindsey Nystrom	T-41G-22	National Cyber Crime Conference - Norwood MA	04/26/ -04/28		$ 32.19					
		TOTAL FOR 4/1/22 -06/30/22		**$ 264.99**	**$ 112.67**	**$ 1,530.00**	**$ -**	**$ -**	**$ -**	**$1,875.47**

"T" Number if Appli		DESCRIPTION	Dates of Travel	B01	B02	B05	B08	B10	C98 - Contracted	Total
Jason Stelmat		Travel to Randolph MA for Shadow Dragon training	7/12/2022		$ -				$44.46	$44.46
Melissa Pirotta		Mileage to National Cyber Crime Conference Norwood, MA	4/26-4/28		$ 115.86					$115 86
Kristin Wilczynski		Texas A&M Engineering Critical Infrastructure Course, Worcester MA	5/5/2022		$ 11.64					$11.64
		TOTAL FOR 7/1/22 - 9/30/22		**$0.00**	**$127.50**	**$0.00**	**$0.00**	**$0.00**	**$44.46**	**$171.96**

"T" Number if Appli		DESCRIPTION	Dates of Travel	B01	B02	B05	B08	B10	C98 - Contracted	Total
Joel Zayas		Travel to Boston, MA for Amtrak/RAILSAFE training	5/16 - 5/17/23						$45.55	$45 55
		TOTAL FOR 7/1/2023 - 9/30/2023		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ 45.55**	**$45.55**
"T" Number if Appli		DESCRIPTION	Dates of Travel	B01	B02	B05	B08	B10	C98 - Contracted	Total
		TOTAL FOR 10/1/23 - 12/31/23		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$0.00**

TOTAL	$ 264.99	$ 240.17	$ 1,530.00	$ -	$ -	$ 90.01	$ 2,092 98

"Other"

2579

Reimbursable Grants Level 2

Menu

	Department	Major Program	Program	Funding Profile	Funding Priority	Funding Line	Obligation Ceiling	Pre Encumbered	Encumbered	Total Expenses
✓	POL	UASI2	FUASI21COM	FEDGRT	1	1	$200 000 00	$0 00	$0 00	$156 157 39

First Prev Next Last

Search

E pense Actuals

Pre Encumbered	$0.00	Obligation Ceiling	$200 000 00
Encumbered	$0 00	E penditure Ceiling	$200 000 00
Advances	$0.00	Uncommitted	$43 842 61
Accrued Expenses	$0 00	Une pended	$43 842 61
Cash E penses	$156,157.39	Back End plits	$0.00
Total Expenses	$156,157.39		
Charges	$0 00		

Revenue Actuals

Unbilled Earned Revenue	$0 00	Collected Earned Revenue	$156 157 39
Billed Earned Revenue	$0.00	Collected Unearned/Deferred Revenue	$0 00
		Total Revenue	$156,157 39
		Revenue Credits	$0 00

Budgetary Amounts

Beginning Balance	$0 00	Revenue Beginning Balance	$0 00
Awarded	$200,000.00	Original Revenue Budget	$0 00
Amendments	$0 00	Revenue Amendments	$0 00
Transfer Out	$0.00	Current Revenue Budget	$0 00
Transfer In	$0 00	Unrecognized Revenue	($156 157 39)
Current Modi ied Budget	$200 000 00	Revenue Balance Forward	$0 00
Balance Forward	$0.00		

General In ormation

Department	POL	Name	FFY21 UASI
Major Program	UASI2	tart Date	11/29/2021
Program	FUASI21COM	End Date	
Funding Pro ile	FEDGRT	Parent Dept	105
Funding Priority	1	Description	EXECUTIVE OFFICE OF PUBLIC SAFETY & HOMELAND SECURITY
Funding Line	1		
		Legal Cite	
		Active	☑

Top

Modified Budget Line Controls Previous Level

THE COMMONWEALTH OF MASSACHUSETTS
TRAVEL AUTHORIZATION FORM (Form TAF)

1. Date of Request:	2. Travel Request #:	3. Department/Division:	4. DEPT/ORGN:	5. Appropriation No.:
5/9/2023		MSP/CIIS	POL	

6. Name of Traveler:	7. Title(s):	8. Dates of Travel:
Joel Zayas	Critical Infrastructure Asset Management Analyst	5/16-5/17 2023

9. Travel Itinerary and Justification

Supporting documentation, i.e. Agendas or brochures.

The Amtrak Police Department RAILSAFE partner training course that is available to select individuals. It is a one and half day program designed to strengthen coordination and integration between Amtrak and partner first responder and emergency management agencies. The course is hosted by Amtrak. The training course is being held in Boston, MA (more details TBD). As the Critical Infrastructure Asset Management Analyst assigned to the Commonwealth Fusion Center's (CFC) Commonwealth Critical Infrastructure Program (CCIP), this training will benefit the Commonwealth as I will be able to use this knowledge to assist critical infrastructure owners and operators in enhancing security and resilience, leading to a more secure Commonwealth.

10. Expenses	Personal Funds	MA State Funds	Federal/ Other State Funds
Transportation: (check all that apply) ☐ Rail ☐Bus ☐Airfare ☑Car: ☐ State ☑Personal ☐Rental ☐Taxi ☐Other:		Mileage 2.4 miles (one way) x 4 = 9.6 miles x .62/mile = $5.95	
Lodging:			
Meals:			
Other: (please list): Parking		Parking $19.80/day = $39.60	
Sub Total(s):			

GRAND TOTAL: $45.55

11. Certifications and Authorizations (See G.L. c. 30, §25B)

I hereby certify under the pains and penalties of perjury that, to the best of my knowledge, the above information is true and correct.
Signature of Traveler: Date: 5/9/2023

I hereby certify that sufficient funds are available for the above described travel accommodations.
Signature of Agency CFO: Date:

I hereby authorize the anticipated travel described above and related expenses listed in this form.
Signature of Traveler's Appointing Authority: Title: Date:

I hereby authorize the anticipated travel described above and related expenses listed in this form.
Signature of the Traveler's Cabinet Secretary Date:

12. Travel Funded By Private Entity, Foreign Government Entity, or Federally Recognized Tribe:

Travel Funded By Private Funds: ☐Yes ☐No
If Yes: $_____ Source (Contact Information):_____

TRAVEL FUNDED BY PRIVATE SOURCES MUST BE DISCLOSED TO AND AUTHORIZED BY APPOINTING AUTHORITY PURSUANT TO 930 CMR 5.08 (2)(d)(1). FOR THE APPROPRIATE FORM GO TO: https://www.mass.gov/disclosure-forms

13: Upon final approval, the Cabinet Secretary shall ensure that a copy of this form is distributed to:
☐ A&F Budget Director & The Office of the Comptroller (please check once complete)

Grant Program Spending Report

Appropriation	Program	BFY	Doc_ID_Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
Dept: POL										
80004794	Urban Areas Initiative Grant									
FUASI21COM	COMM CRITICAL INFRASTRUCTURE PROG									
		2022								
object_class	BB									
B01	Other Out Of State Travel - INCLUSIVE: AIRFARE, HOTEL, LODGI									
PREXP	POL		EMPL 020220521151648			$118.17			5/24/2022	5/24/2022	5/24/2022
Summary for 'Object' = B01 (1 detail record)						*$118.17*				
B02	In-State Travel									
PREXP	POL		EMPL 020220507136928			$127.32			5/10/2022	5/10/2022	5/10/2022
PRADJ	POL		05162200000000014534			$19.50			5/16/2022	5/16/2022	5/16/2022
PREXP	POL		EMPL 020220604124648			$80.48			6/7/2022	6/7/2022	6/7/2022
PREXP	POL		EMPL 020220604162448			$32.19			6/7/2022	6/7/2022	6/7/2022
PREXP	POL		EMPL 020220730150188			$127.50			8/2/2022	8/2/2022	8/2/2022
Summary for 'Object' = B02 (5 detail records)						*$386.99*				
B05	Conference, Training, Registration and Membership Dues and L									
PREXP	POL		EMPL 020220507136928			$790.00			5/10/2022	5/10/2022	5/10/2022
PREXP	POL		EMPL 020220521151648			$345.00			5/24/2022	5/24/2022	5/24/2022
PREXP	POL		EMPL 020220604124648			$282.14			6/7/2022	6/7/2022	6/7/2022
PREXP	POL		EMPL 020220604162448			$112.86			6/7/2022	6/7/2022	6/7/2022
PREXP	POL		EMPL 020220730150188			$395.00			8/2/2022	8/2/2022	8/2/2022
Summary for 'Object' = B05 (5 detail records)						*$1,925.00*				
Summary for 'Object_Class' = BB (11 detail records)						*$2,430.16*				
object_class	UU									
U10	Information Tech (IT) Equipment Maintenance & Repair									
PRC	POL	7214	PVPOL721422103INS652	VC6000239916	INSIGHT PUBLIC SECTOR INC	1100928715	4/4/2022	$23,845.33	$0.00	$23,845.33	3/30/2022	3/30/2022	4/14/2022
Summary for 'Object' = U10 (1 detail record)								*$23,845.33*	*$0.00*	*$23,845.33*			
U12	Information Tech (IT) cloud services									
PRC	POL	7214	PVPOL721422686SHI643	VC6000227588	SHI INTERNATIONAL CORP	B15199808	5/10/2022	$3,157.00	$0.00	$3,157.00	5/12/2022	6/30/2022	7/5/2022
Summary for 'Object' = U12 (1 detail record)								*$3,157.00*	*$0.00*	*$3,157.00*			
Summary for 'Object_Class' = UU (2 detail records)								*$27,002.33*	*$0.00*	*$27,002.33*			
Summary for 'budget_fiscal_year' = 2022 (13 detail records)								*$29,432.49*	*$0.00*	*$27,002.33*			
		2023								
object_class	CC									
C23	Management, Business Professionals & Admin Services									
PRADJ	POL		08232200000000004534			$1,600.00			8/23/2022	8/23/2022	8/30/2022
PRADJ	POL		08232200000000004538			$3,200.00			8/23/2022	8/23/2022	8/30/2022
PRADJ	POL		08232200000000004536			$3,200.00			8/23/2022	8/23/2022	8/30/2022
PREXP	POL		CNTR 020220827105758			$3,200.00			8/30/2022	8/30/2022	8/30/2022
PREXP	POL		CNTR 020220910105568			$2,880.00			9/13/2022	9/13/2022	9/13/2022
PREXP	POL		CNTR 020220924103947			$3,200.00			9/27/2022	9/27/2022	9/27/2022
PREXP	POL		CNTR 020221008106718			$2,560.00			10/11/2022	10/11/2022	10/11/2022
PREXP	POL		CNTR 020221022107728			$2,880.00			10/25/2022	10/25/2022	10/25/2022
PREXP	POL		CNTR 020221105107438			$3,200.00			11/8/2022	11/8/2022	11/8/2022
PREXP	POL		CNTR 020221119107038			$2,880.00			11/22/2022	11/22/2022	11/22/2022
PREXP	POL		CNTR 020221203108548			$2,880.00			12/6/2022	12/6/2022	12/6/2022
PREXP	POL		CNTR 020221217106868			$3,200.00			12/20/2022	12/20/2022	12/20/2022
PREXP	POL		CNTR 020221231104538			$3,200.00			1/3/2023	1/3/2023	1/3/2023
PREXP	POL		CNTR 020230114102258			$2,820.00			1/17/2023	1/17/2023	1/17/2023
PREXP	POL		CNTR 020230128106388			$3,400.50			1/31/2023	1/31/2023	1/31/2023

Appropriation	Program	BFY	Doc_ID_Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
2582										
PREXPPOL	CNTR 020230211107098					$3,280.00			2/14/2023 2/14/2023	2/14/2023
PREXPPOL	CNTR 020230225106878					$1,824.50			2/28/2023 2/28/2023	2/28/2023
PREXPPOL	CNTR 020230311106278					$3,239.00			3/14/2023 3/14/2023	3/14/2023
PREXPPOL	CNTR 020230325107088					$3,280.00			3/28/2023 3/28/2023	3/28/2023
PREXPPOL	CNTR 020230408106488					$3,280.00			4/11/2023 4/11/2023	4/11/2023
PREXPPOL	CNTR 020230422102938					$3,198.00			4/25/2023 4/25/2023	4/25/2023
PREXPPOL	CNTR 020230506106968					$3,280.00			5/9/2023 5/9/2023	5/9/2023
PREXPPOL	CNTR 020230520105278					$3,116.00			5/23/2023 5/23/2023	5/23/2023
PREXPPOL	CNTR 020230603106708					$3,280.00			6/6/2023 6/6/2023	6/6/2023
PREXPPOL	CNTR 020230617106768					$3,136.50			6/20/2023 6/20/2023	6/20/2023
PREXPPOL	CNTR 020230701103687					$3,239.00			7/4/2023 7/4/2023	7/4/2023
Summary for 'Object' = C23 (26 detail records)						*$78,453.50*				
C98 Reimb Travel/Other Expenses CC Special Contract/Employee										
PREXPPOL	CNTR 020220730106218					$44.46			8/2/2022 8/2/2022	8/2/2022
PREXPPOL	CNTR 020230715103598					$45.55			7/18/2023 7/18/2023	7/18/2023
Summary for 'Object' = C98 (2 detail records)						*$90.01*				
Summary for 'Object_Class' = CC (28 detail records)						*$78,543.51*				
object_class DD										
D09 Fringe Benefit Cost Recoupment										
CA CTR	PTXOPYTX0910220000008625					$207.20				9/10/2022
CA CTR	PTXOPYTX1009220000011175					$112.48				10/9/2022
CA CTR	PTXOPYTX1106220000013707					$100.64				11/6/2022
CA CTR	PTXOPYTX1210220000016234					$112.48				12/10/2022
CA CTR	PTXOPYTX0107230000018838					$112.48				1/7/2023
CA CTR	PTXOPYTX0204230000021581					$174.28				2/4/2023
CA CTR	PTXOPYTX0304230000024225					$94.43				3/4/2023
CA CTR	PTXOPYTX0408230000026704					$120.60				4/8/2023
CA CTR	PTXOPYTX0506230000029204					$119.84				5/6/2023
CA CTR	PTXOPYTX0610230000031704					$118.33				6/10/2023
CA CTR	PTXOPYTX0708230000002348					$178.63				7/8/2023
Summary for 'Object' = D09 (11 detail records)						*$1,451.39*				
Summary for 'Object_Class' = DD (11 detail records)						*$1,451.39*				
object_class EE										
EE2 Conference, Training and Registration Fees										
GAX POL 7214	PVPOL721422194SANS01		VC6000249640	ESCAL INSTITUTE OF ADVANCED TECAGGREGATE-73885-1118969	14/2022	$37,098.00	$0.00	$37,098.00	7/13/2022 7/13/2022	7/15/2022
Summary for 'Object' = EE2 (1 detail record)						*$37,098.00*	*$0.00*	*$37,098.00*		
Summary for 'Object_Class' = EE (1 detail record)						*$37,098.00*	*$0.00*	*$37,098.00*		
Summary for 'budget_fiscal_year' = 2023 (40 detail records)						*$117,092.90*	*$0.00*	*$37,098.00*		
2024										
object_class CC										
C23 Management, Business Professionals & Admin Services										
PREXPPOL	CNTR 020230715103388					$3,096.00			7/18/2023 7/18/2023	7/18/2023
PREXPPOL	CNTR 020230729102978					$3,096.00			8/1/2023 8/1/2023	8/1/2023
PREXPPOL	CNTR 020230812102518					$3,440.00			8/15/2023 8/15/2023	8/15/2023
Summary for 'Object' = C23 (3 detail records)						*$9,632.00*				
Summary for 'Object_Class' = CC (3 detail records)						*$9,632.00*				
Summary for 'budget_fiscal_year' = 2024 (3 detail records)						*$9,632.00*				
Summary for 'Program' = FUASI21COM (56 detail records)						*$156,157.39*	*$0.00*	*$64,100.33*		
Summary for 'Appropriation' = 80004794 (56 detail records)						*$156,157.39*	*$0.00*	*$64,100.33*		
Summary for 'Department' = POL (56 detail records)						*$156,157.39*	*$0.00*	*$64,100.33*		

Appropriation_Program	BFY	Doc_ID_Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
2585									
Grand Total					$156,157.39	$0.00	$64,100.33		

Form Name: 2584
Submission Time: HLS Quarterly Report
Browser: October 13, 2023 11:20 am
IP Address: Chrome 117.0.0.0 / Windows
Unique ID: 170.63.192.1
Location: 1152008876

Which subrecipient are you reporting data for in this quarterly progress report?	Other Agency
Please select which other agency you are reporting data for in this quarterly report.	MSP Commonwealth Fusion Center (CFC)

Reporting Information

Project Name	FUASI21COM
Federal Fiscal Year (FFY) Funding	FFY 2021

Contact Information

Reported by	Amy Thibault
Job Title	Intelligence Services Manager
Email Address	amy.thibault@pol.state.ma.us
Phone Number	(978) 451-3717

Reporting Period

Quarter Number	3
Reporting Period (Months)	July 1st - September 30th
Reporting Period (Year)	2023

Instructions

I. Planning

II. Organization

Regional Specialty Response Teams

III. Equipment

IV. Training

Exercise Program

Type of exercise	Seminar

V. Management and Administration

Management and Administration Text	We worked with SITE Intel Group on their terms and conditions in order to ensure that we could use the information in CCIP products prior to moving ahead with a subscription.

VI. Other Activities

VII. Challenges/Delays

VIII. Success Stories

IX. Meetings

Waste, Fraud, or Abuse

Are you aware of any concerns regarding waste, fraud, or abuse connected to any of the grant-funded activities described in this report?	No

Fiduciary Coordinator Signature

Electronic Signature



Date	Oct 13, 2023

Submitting Your QR

Massachusetts Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Grant Division

QUARTERLY FINANCIAL REPORT

Agency/Contractor Name:	Massachusetts State Police	**Date:**	Friday, October 6, 2023
Project Name:	FFY22 Commonwealth Critical Infrastructure Program	**E-mail:**	jeff.ly@pol.state.ma.us
Grant Program & FFY:	FUASI22CIP 8000-4794	**Telephone:**	508-988-7081
Reported by:	Jeff Ly	**FAX:**	508-820-2165

Report Number	Reporting Period	Year	Report Due
Quarter _X_	July 1st – September 30th	2023	October 15th
Quarter ___	October 1st – December 31st	2023	January 15th
Quarter ___	January 1st – March 31st	2024	April 15th
Quarter ___	April 1st – June 30th	2024	July 15th

SUMMARY OF COSTS

Expense Category	Approved Budget	Expended This Quarter	Expended to Date	Obligated to Date	Balance	% Remaining
Salary	$0.00	$0.00	$0.00	$0.00	0.00	0%
Fringe	$1,651.10	$0.00	$0.00	$0.00	1,651.10	100%
Indirect	$0.00	$0.00	$0.00	$0.00	0.00	0%
Consultants/Contracts	$87,360.00	$9,632.00	$9,632.00	$0.00	77,728.00	89%
Travel	$15,000.00	$0.00	$0.00	$0.00	15,000.00	100%
Equipment	$0.00	$0.00	$0.00	$0.00	0.00	0%
Supplies	$3,711.90	$0.00	$0.00	$0.00	3,711.90	100%
Overtime	$0.00	$0.00	$0.00	$0.00	0.00	0%
Other (software, registrations, seminars)	$92,277.00	$0.00	$46,171.69	$0.00	$46,105.31	50%
TOTAL	**$200,000.00**	**$9,632.00**	**$55,803.69**	**$0.00**	**$144,196.31**	72%

Reports must be submitted for every full or partial calendar quarter during the grant period regardless of spending activity.

Please send this report along with the Quarterly Financial Detail and Quarterly Progress Reports to:

Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720A

Boston, MA 02116
ATTN: Vicky Mboka-Boyer *via email*

Rebecca Rust
Authorized Signature (Blue ink please)

10/11/23
Date

Rebecca Rust
Print Name

Executive Office of Public Safety

Quarterly Financial Report (Detail for Expenditures)

Quarter Reporting Period (Choose From Cell Below): 7/1-9/30

Year Reporting Period (Choose From Cell Below): 2023

FFY 2022 FUASI22CIP

Salary:Please List all Employees charged to grant along with either: hours and rate, if paid hourly; or amount paid to employee for period from federal funds and a brief description, if salaried

Employee Name	Hrs/Unit	Rate/Amt	Description	Total	
				Sub-Total:	$0.00

Fringe: Fringe costs must go by Federally approved rate, and base amount should easily be identified from this detailed report.

Employee Name	Approved Rate	Base Amount			
				Sub-Total:	$0.00

Indirect: Indirect Rate must be a federally Negotiated and approved rate, and base amount should easily be identified from this detailed report.

Employee/Contracted Employee Name	Approved Rate	Base Amount		Total	
				Sub-Total:	$0.00

Consultants/Contracts: Please list Name of Consultant or Entity contract is with, hours and rate of contract and a brief description. If total costs for quarter for any single contract exceed $5K, please provide invoices

Company/Name	Hours	Rate	Description	Total	
Zayas, Joel	80	$ 43.00	Payroll for pay period end date 08/26/22	$3,440.00	
Zayas, Joel	72	$ 43.00	Payroll for pay period end date 09/9/22	$3,096.00	
Zayas, Joel	72	$ 43.00	Payroll for pay period end date 09/23/22	$3,096.00	
				Sub-Total:	$9,632.00

Travel: Please list each employee, cost of travel, description/purpose of travel, and the guidelines followed for reimbursement (Local, State, or Federal). Please include all receipts.

Employee Name	Cost	Guidelines	Purpose/Description	Total	Receipt Y/N
				Sub-Total:	$0.00

Piece of equipment	Unit Cost	Quantity	Description of Equipment	Total	Receipt
				Sub-Total:	$0.00

Supplies: Please list supplies and computation basis for reimbursement request.

Item	Cost		Basis for Computation	Total	
				Sub-Total:	$0.00

Overtime

Employee Name	Hrs/Unit	Rate/Amt	Description	Total	
				Sub-Total:	$0.00

Other: Please list Item and Basis for Computation.

Item	Cost	Qty	Basis for Computation	Total	Receipt
				Sub-Total:	$0.00

Total:

Total:*	$9,632.00

Program:	**FUASI22CIP**											
Appropriation:	**8000-4794**											
department	pay_period end date	employee id	employee name	title_description	event type	event_type_description	SumOfinput amount	AMOUNT	object	object_description	appropriation	program
POL	26-Aug-23	540564	Zayas, Joel G	Program Coordinators	REC	CONTRPAY	80	$ 3,440.00	C23	Mgnt&Admn-SVS	80004794	FUASI22CIP
POL	23-Sep-23	540564	Zayas, Joel G	Program Coordinators	REC	CONTRPAY	72	$ 3,096.00	C23	Mgnt&Admn-SVS	80004794	FUASI22CIP
POL	09-Sep-23	540564	Zayas, Joel G	Program Coordinators	REC	CONTRPAY	72	$ 3,096.00	C23	Mgnt&Admn-SVS	80004794	FUASI22CIP
						PAYROLL 9/30/23 -		$ 9,632.00	✓			
								$ 9,632.00	C23	CONSULTANTS/CONTRACTS		
								$ -	C98	TRAVEL		

2589

Program: FUASI22CIP
Appropriation: 8000-4797

fiscal year	department	doc_code	cash_expense amount	service_from date	service_to date	appropriation	object	object_name	vendor_customer code	legal_name	program	acceptance date
2023	POL	EFT	$ 3,462.11	15-Jan-23	15-Jan-23	80004794	U10	Information Tech (IT) Equipment	VC6000227588	SHI INTERNATIONAL CORP	FUASI22CIP	24-Feb-23
	Expenditures 3/31/23		$ 3,462.11									
2023	POL	EFT	$ 25,538.63	16-Feb-23	16-Feb-23	80004794	U10	Information Tech (IT) Equipment	VC6000239916	INSIGHT PUBLIC SECTOR INC	FUASI22CIP	12-Apr-23
2023	POL	EFT	$ 3,148.95	12-May-23	12-May-23	80004794	U12	Information Tech (IT) cloud servic	VC6000227588	SHI INTERNATIONAL CORP	FUASI22CIP	21-Jun-23
2023	POL	AD	$ 14,022.00	23-Jun-23	23-Jun-23	80004794	EE2	Conference, Training and Registra	VC6000249640	ESCAL INSTITUTE OF ADVANC	FUASI22CIP	23-Jun-23
	Expenditures 6/30/23		$ 42,709.58									
2024	POL	PRLNP	$ 3,440.00	45167	45167	80004794	C23	Management, Business Professio			FUASI22CIP	45167
2024	POL	PRLNP	$ 3,096.00	45181	45181	80004794	C23	Management, Business Professio			FUASI22CIP	45181
2024	POL	PRLNP	$ 3,096.00	45195	45195	80004794	C23	Management, Business Professio			FUASI22CIP	45195
	Expenditures 9/30/23		$ 9,632.00	✓								
		TOTAL	$ 55,803.69	✓								

2590

Reimbursable Grants Level 2

Menu

Department	Major Program	Program	Funding Profile	Funding Priority	Funding Line	Obligation Ceiling	Pre Encumbered	Encumbered	Total Expenses
POL	UASI2	FUASI22C P	FEDGRT	1	1	$200 000 00	$0 00	$0 00	$55 803 69

First Prev Next Last

Search

E pense Actuals

Pre Encumbered	$0.00	Obligation Ceiling	$200 000 00
Encumbered	$0 00	E penditure Ceiling	$200 000 00
Advances	$0.00	Uncommitted	$144 196 31
Accrued Expenses	$0 00	Une pended	$144 196 31
Cash E penses	$55,803 69	Back End plits	$0.00
Total Expenses	$55,803 69		
Charges	$0 00		

Revenue Actuals

Unbilled Earned Revenue	$0 00	Collected Earned Revenue	$52 707 69
Billed Earned Revenue	$3,096.00	Collected Unearned/De erred Revenue	$0 00
		Total Revenue	$55,803 69
		Revenue Credits	$0 00

Budgetary Amounts

Beginning Balance	$0 00	Revenue Beginning Balance	$0 00
Awarded	$200,000.00	Original Revenue Budget	$0 00
Amendments	$0 00	Revenue Amendments	$0 00
Trans er Out	$0.00	Current Revenue Budget	$0 00
Transfer In	$0 00	Unrecognized Revenue	($55 803 69)
Current Modi ied Budget	$200 000 00	Revenue Balance Forward	$0 00
Balance Forward	$0.00		

General In ormation

Department	POL	Name	FFY22 UASI
Major Program	UASI2	tart Date	01/11/2023
Program	FUASI22C P	End Date	
Funding Pro ile	FEDGRT	Parent Dept	105
Funding Priority	1	Description	EXECUTIVE OFFICE OF PUBLIC SAFETY & HOMELAND SECURITY
Funding Line	1		
		Legal Cite	
		Active	☑

Top

Modified Budget Line Controls Previous Level

Grant Program Spending Report

Appropriation	Program	BFY	Doc_ID_Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
Dept: POL										
80004794	Urban Areas Initiative Grant									
FUASI22CIP	COMM CRITICAL INFRASTRUCTURE PROG.									
		2023								
object_class	EE									
EE2	Conference, Training and Registration Fees									
GAX	POL 7214		GAXPOL721423SANS0001	VC6000249640	ESCAL INSTITUTE OF ADVANCED TECAGGREG-79015-12242070 6/23/2023	$14,022.00	$0.00	$14,022.00	6/23/2023	6/23/2023	6/23/2023
Summary for 'Object' = EE2 (1 detail record)						*$14,022.00*	*$0.00*	*$14,022.00*			
Summary for 'Object_Class' = EE (1 detail record)						*$14,022.00*	*$0.00*	*$14,022.00*			
object_class	UU									
U10	Information Tech (IT) Equipment Maintenance & Repair									
PRC	POL 7214		PVPOL72142331SHI9012	VC6000227588	SHI INTERNATIONAL CORP B16329012 1/10/2023	$3,462.11	$0.00	$3,462.11	1/15/2023	1/15/2023	2/6/2023
PRC	POL 7214		PVPOL72142394INSIG34	VC6000239916	INSIGHT PUBLIC SECTOR INC 1101031134 3/1/2023	$25,538.63	$0.00	$25,538.63	2/16/2023	2/16/2023	4/5/2023
Summary for 'Object' = U10 (2 detail records)						*$29,000.74*	*$0.00*	*$29,000.74*			
U12	Information Tech (IT) cloud services									
PRC	POL 7214		PVPOL721423130SHI001	VC6000227588	SHI INTERNATIONAL CORP B16574926 5/10/2023	$3,148.95	$0.00	$3,148.95	5/12/2023	5/12/2023	5/15/2023
Summary for 'Object' = U12 (1 detail record)						*$3,148.95*	*$0.00*	*$3,148.95*			
Summary for 'Object_Class' = UU (3 detail records)						*$32,149.69*	*$0.00*	*$32,149.69*			
Summary for 'budget_fiscal_year' = 2023 (4 detail records)						*$46,171.69*	*$0.00*	*$46,171.69*			
		2024								
object_class	CC									
C23	Management, Business Professionals & Admin Services									
PREXP	POL		CNTR 020230826102198			$3,440.00			8/29/2023	8/29/2023	8/29/2023
PREXP	POL		CNTR 020230909105668			$3,096.00			9/12/2023	9/12/2023	9/12/2023
PREXP	POL		CNTR 020230923104268			$3,096.00			9/26/2023	9/26/2023	9/26/2023
Summary for 'Object' = C23 (3 detail records)						*$9,632.00*					
Summary for 'Object_Class' = CC (3 detail records)						*$9,632.00*					
Summary for 'budget_fiscal_year' = 2024 (3 detail records)						*$9,632.00*					
Summary for 'Program' = FUASI22CIP (7 detail records)						*$55,803.69*	*$0.00*	*$46,171.69*			
Summary for 'Appropriation' = 80004794 (7 detail records)						*$55,803.69*	*$0.00*	*$46,171.69*			
Summary for 'Department' = POL (7 detail records)						*$55,803.69*	*$0.00*	*$46,171.69*			

Appropriation_Program	BFY	Doc_ID_Code	Vendor Code /Name	Vendor Inv No /Date	Ln_Amt	Disc_Amt	Chk_Amt	Srvc_From/To_Dt	Accpt_Dt
2592									
Grand Total					*$55,803.69*	*$0.00*	*$46,171.69*		

Form Name: 2593
Submission Time: HLS Quarterly Report
October 13, 2023 11:25 am
Browser: Chrome 117.0.0.0 / Windows
IP Address: 170.63.192.1
Unique ID: 1152010644
Location:

Which subrecipient are you reporting data for in this quarterly progress report?	Other Agency
Please select which other agency you are reporting data for in this quarterly report.	MSP Commonwealth Fusion Center (CFC)

Reporting Information

Project Name	FUASI22CIP
Federal Fiscal Year (FFY) Funding	FFY 2022

Contact Information

Reported by	Amy Thibault
Job Title	Intelligence Services Manager
Email Address	amy.thibault@pol.state.ma.us
Phone Number	(978) 451-3717

Reporting Period

Quarter Number	3
Reporting Period (Months)	July 1st - September 30th
Reporting Period (Year)	2023

Instructions

I. Planning

II. Organization

Regional Specialty Response Teams

III. Equipment

IV. Training

Exercise Program

Type of exercise	Seminar

V. Management and Administration

VI. Other Activities

VII. Challenges/Delays

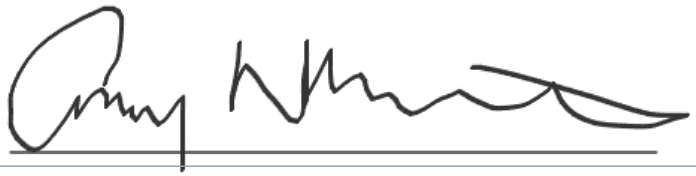
VIII. Success Stories

IX. Meetings

Waste, Fraud, or Abuse

Are you aware of any concerns regarding waste, fraud, or abuse connected to any of the grant-funded activities described in this report?	No

Fiduciary Coordinator Signature

Electronic Signature	
Date	Oct 13, 2023

Submitting Your QR

AirLink® RV55: Industrial LTE-A Pro Router

The AirLink® RV55 delivers LTE and Wi-Fi connectivity for vehicles and remote fixed assets operating in harsh environments. With ultra-low power consumption, the RV55 is ideal for solar/battery powered installations.

AirLink® RV55
Rugged LTE-A Pro router capable of 600Mbps download and 150 Mbps upload. Wi-Fi optional.





AirLink® RV55 – Router Specifications

	North America	EMEA	Global
CELLULAR			
Peak D/L	**RV55 LTE** – Up to 150 Mbps, Cat 4 (WP7610 | WP7607) **RV55 LTE-A PRO** – Up to 600 Mbps, Cat 12 (EM7511 | EM7565)	**RV55 LTE** – Up to 150 Mbps, Cat 4 (WP7610 | WP7607) **RV55 LTE-A PRO** – Up to 600 Mbps, Cat 12 (EM7511 | EM7565)	**RV55 LTE** – Up to 150 Mbps, Cat 4 (WP7610 | WP7607) **RV55 LTE-A PRO** – Up to 600 Mbps, Cat 12 (EM7511 | EM7565)
Peak U/L	**RV55 LTE** – Up to 50 Mbps **RV55 LTE-A PRO** – Up to 150 Mbps	**RV55 LTE** – Up to 50 Mbps **RV55 LTE-A PRO** – Up to 150 Mbps	**RV55 LTE** – Up to 50 Mbps **RV55 LTE-A PRO** – Up to 150 Mbps
4G LTE			
Frequency Bands	**RV55 LTE** – 1900(B2), AWS(B4), 850(B5), 700(B12), 700(B13), 700(B17), 1700(B66) **RV55 LTE-A PRO** – 2100(B1), 1900(B2),1800(B3), AWS(B4), 850(B5), 2600(B7), 900(B8), 1800(B9), 700(B12), 700(B13), 700(B14), 850(B18), 850(B19), 800(B20), 850(B26), 700(B29), 2300(B30), 1500(B32), TDD B41, TDD B42, TDD B43, TDD B46, CBRS B48,1700(B66)	**RV55 LTE** – 2100(B1), 1800(B3), 2600(B7), 900(B8), 800(B20), 700(B28)	**RV55 LTE-A PRO** – 2100(B1), 1900(B2), 1800(B3), AWS(B4), 850(B5), 2600(B7), 900(B8), 1800(B9), 700(B12), 700(B13), 850(B18), 850(B19), 800(B20), 850(B26), 700(B28), 700(B29), 2300(B30), 1500(B32), TDD B41, TDD B42, TDD B43, TDD B46, CBRS B48, 1700(B66)

3G HSPA/HSPA+

Frequency Bands*	**RV55 LTE** – 1900(B2), AWS(B4), 850(B5) **RV55 LTE-A PRO** – 2100(B1), 1900(B2), AWS(B4), 850(B5), 800(B6), 900(B8), 1700(B9), 850(B19)	**RV55 LTE** – 2100(B1), 900(B8)	**RV55 LTE-A PRO** – 2100(B1), 1900(B2), AWS(B4), 850(B5), 800(B6), 900(B8), 1700(B9), 850(B19)

2G EDGE/GSM/GPRS

Frequency Bands		**RV55 LTE** – 900, 1800	**RV55 LTE-A PRO** – 850, 900, 1800, 1900

APPROVALS

Regulatory**	**RV55 LTE** – FCC, IC, PTCRB **RV55 LTE-A PRO** – FCC, IC, PTCRB	**RV55 LTE** – GCF, CE	**RV55 LTE-A PRO** – FCC, IC, PTCRB, GCF, CE, RCM, IFT, Anatel
Carrier**	**55 LTE** – Verizon, AT&T, T-Mobile **RV55 LTE-A PRO** – Verizon, AT&T/FirstNet, US Cellular, T-Mobile, Telus, Rogers, Bell, Southern Linc		**RV55 LTE-A PRO** – Verizon, AT&T, Telstra (Planned)

PART NUMBER

Part Number	**RV55 LTE** – 1104335 **RV55 LTE-A PRO** – 1104303, 1104302 (Wi-Fi), 1104302 (Wi-Fi)	**RV55 LTE** – 1104337	**RV55 LTE-A PRO** – 1104332, 1104331 (Wi-Fi), 1104331 (Wi-Fi)

**For carrier-specific band support please refer to the hardware user guide.*
***All approvals are either granted or in progress. Call for the latest approval status.*

HOST INTERFACES

10/100/1000 Ethernet (RJ45)
RS-232 serial port (DB-9)
USB 2.0 Micro-B Connector
3 SMA antenna (cellular, diversity, GNSS)
2 RP-SMA antenna (1×1 Wi-Fi, Optional)
Active GPS antenna support

SECURITY

Remote Authentication (LDAP, RADIUS, TACACS+, DMZ)
Inbound and Outbound Port filtering
Inbound and Outbound Trusted IP
MAC Address Filtering
PCI compatible
Secure Firmware Update

WI-FI (OPTIONAL)

	Dual Band 2.4/5GHz Wi-Fi Dual Radio, 802.11 b/g/n/ac (Wave2 Client Mode) Support for 10 clients, WPA2 Enterprise per radio Output power 16dBm Configurable as Dual Band Access Point (AP) or AP+Client Mode Single SSID Support per radio Captive Portal

SATELLITE NAVIGATION (GNSS)

	LTE-A Pro Variant: 30 Channel GPS and GLONASS Receiver (Tracking Sensitivity: -160dBm) LTE Variant: 48 Channel Dedicated GNSS Receiver (Tracking Sensitivity: -162 dBm) Accuracy: <2 m (50%), <5 m (90%), <0.2 m/s Acquisition Time: 1s Hot Start Reports: NMEA 0183 V3.0, TAIP, RAP, XORA Multiple Redundant Servers Reliable Store and Forward

ENVIRONMENTAL

Operating Temperature	-40°C to +70°C / -40°F to +158°F
Operating Temperature (Wi-Fi variant)	-30°C to +70°C / -22°F to +158°F
Storage Temperature	-40°C to +85°C / -40°F to +185°F
Humidity	95% RH @ 60°C
	Military Spec MIL-STD-810G conformance to shock, vibration, thermal shock, and humidity IP64 rated ingress protection

POWER

Input/Operating Voltage	**Input Voltage:** 7 to 36 VDC Configurable I/O pin on power connector Digital Input ON Voltage: 2.7 to 36 VDC Configurable Pull-up for dry contact input Digital Open Collector Output > sinking 500 mA Analog Input: 0.5-36 VDC
Power Modes	**Idle Power:** 900mW (75 mA @ 12VDC) **Standby Mode Power:** 53 mW (4.4 mA @ 12 VDC) triggered on low voltage, I/O or periodic timer Low voltage disconnect to prevent battery drain Built-in protection against voltage transients including 5 VDC engine cranking and +200 VDC load dump Ignition Sense with time delay shutdown Configurable features and ports to optimize power consumption

NETWORK AND ROUTING

	Network Address Translation (NAT) Reliable Static Route Port Forwarding Dynamic DNS Policy Routing Verizon PNTM NEMO/DMNR IPV6 Gateway VRRP

VPN**	
	IPsec, GRE, and OpenVPN Client Up to 5 concurrent tunnels Split Tunnel Dead Peer Detection (DPD) FIPS 140-2 compatible

INDUSTRY CERTIFICATION	
Safety	IECEE Certification Bodies Scheme (CB Scheme), UL 60950****
Vehicle Usage	E Mark (UN ECE Regulation 10 04)
Environmental	RoHS, REACH, WEEE **Hazardous Environments:** Class 1 Div 2 Ambient temperatures of 30°C to +60°C
Rail Usage	EN50155, ISO7637 2, SAE J1455 (Shock & Vibration)

SUPPORT AND WARRANTY	
	1 year standard warranty with up to 5 years extended warranty with current AirLink Complete subscription. Unrestricted critical firmware updates

LAN (ETHERNET/USB)	
	DHCP Server Host Interface Watchdog IP Passthrough PPPoE VLAN

SERIAL	
	TCP/U DP PAD Mode Modbus (ASCII, RTU, Variable) PPP DNP3 Interoperability Dual Serial option (with an accessory)

APPLICATION FRAMEWORK	
	ALEOS Application Framework (AAF) LUA Scripting Language

NETWORK MANAGEMENT	
	Secure mobile network & asset management application available in the cloud or licensed platform in the enterprise data center Fleet wide firmware upgrade delivery Router configuration and template management Router staging over the air and local Ethernet connection Over the air software and radio module firmware updates Device Configuration Templates Configurable monitoring and alerting Remote provisioning and airtime activation (where applicable)

ROUTER MANAGEMENT

	ALMS Local web user interface AT Command Line Interface (Telnet/SSH/Serial) SMS Commands SNMP

EVENTS ENGINE

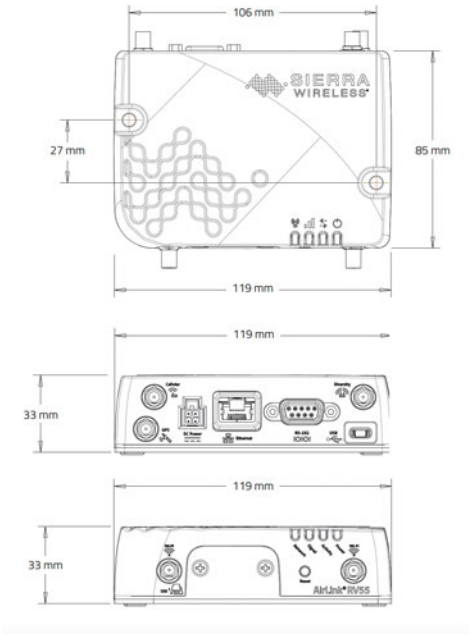
	Custom event triggers and reports Configurable interface, no programming
Event Types	Digital Input, Network Parameters, Data Usage, Timer, Power, Device Temperature and Voltage
Report Types	RAP, SMS, Email, SNMP Trap, TCP (Binary, XML, CSV)
Event Actions	Drive Relay Output

ACCESSORIES

In The Box	RV55, DC Power Cable, and Quick Start Guide
Other Accessories (Sold Separately)	2000579 AC Adapter, 12VDC 6000659 DIN Rail Bracket For Antenna options visit: sierrawireless.com/antennas

DIMENSIONS

AirLink RV55 Main Body	119 mm x 33 mm x 85 mm (102 mm including wi fi connectors) 4.69 in x 1.34 in x 3.35 in (3.70 in including connectors) Weight: 320 g



**For carrier specific band support please refer to the hardware user guide*
***All approvals are either granted or in progress. Call for the latest approval status*
**** IPsec, GRE and OpenVPN Client are not available in the member states of the EAEU*
***** Ambient temperatures of -30C to +60C*

ITC71: Security, Surveillance, Monitoring, and Access Control System

UPDATED: October 13, 2022

Contract #:	ITC71
MMARS MA #:	ITC71*
Initial Contract Term:	June 1, 2019 – May 31, 2024
Maximum End Date:	Two (2), two-year extensions to 2028
Current Contract Term:	June 1, 2019 – May 31, 2024
Contract Manager:	Amanda Ferdinand, 617-720-3166, Amanda.Ferdinand@mass.gov
This Contract Contains:	Prompt Payment Discounts (PPD) Supplier Diversity Office (SDO) Vendors
UNSPSC Codes:	46-17-00 Security surveillance and detection

***The asterisk is required when referencing the contract in the Massachusetts Management Accounting Reporting System (MMARS).**

Table of Contents:

(NOTE: To access hyperlinks below, scroll over desired section and CTL + Click)

- Contract Summary
- Contract Categories
- Benefits and Cost Savings
- Who Can Use This Contract
- Subcontractors
- Construction Requirements
- Supplier Diversity Requirements
- Pricing, Quotes and Purchase Options
- Instructions for MMARS Users
- Emergency Services
- Shipping/Delivery/Returns
- Additional Information/FAQ's
- Strategic Sourcing Team Members
- VENDOR LIST AND INFORMATION
- Appendix A: ITC71 Regions Map
- Appendix B: Contract Categories

TIP: To return to the first page throughout this document, use the CTL + Home command.

Contract Summary

This is a Statewide Contract for Security surveillance and detection. This contract covers the acquisition of Security Systems and Related Services to include, but not limited to, Video, Access Control, Integrated Video Management, Visitor Management, Locks, Alarms, Monitoring Services/Systems, Catalog Sales, Service, and Maintenance.

Contract Categories

This contract includes 4 categories as listed below.

Category 1: Catalog Sales
Category 2: Security Systems Integration (Equipment and Related Services)
Category 3: Security Systems Monitoring Services
Category 4: Locks, Locksmiths, Door Closures, and Related Hardware

Benefits and Cost Savings

Statewide contracts are an easy way to obtain benefits for your organization by leveraging the Commonwealth's buying power, solicitation process, contracting expertise, vendor management and oversight, and the availability of environmentally preferable products.

- Competitive discounts on a wide range of security products
- Competitive hourly wage rates and markups over prevailing wage
- Prompt payment discount opportunities
- Certified Supplier Diversity Office vendors
- Multiple vendors in each category for competition
- Ability to add new products/manufacturers that fit the scope of the RFR

Find Bid/Contract Documents

- To find all contract-specific documents, including the Contract User Guide, RFR, specifications, price sheets and other attachments, visit COMMBUYS.com and search for ITC71 to find related Master Blanket Purchase Order (MBPO) information.
- To find all contract-specific documents, including the Contract User Guide, RFR, specifications, and other attachments, visit COMMBUYS.com and search for ITS71 to find related Master Blanket Purchase Order (MBPO's) information. All common contract documents are located in the "Master Contract Record" Master Blanket Purchase Order (MBPO) for ITC71 and can be accessed directly by visiting Master Blanket Purchase Order PO-19-1080-OSD03-SRC3-16463.

Who Can Use This Contract

Applicable Procurement Law

Executive Branch Goods and Services: MGL c. 7, § 22; c. 30, § 51, § 52; 801 CMR 21.00;

Eligible Entities

Please see the standard list of Eligible Entities on our Eligible Entities Which May Use Statewide Contracts webpage.

Subcontractors

The awarded vendor's use of subcontractors is subject to the provisions of the Commonwealth's Terms and Conditions and Standard Contract Form, as well as other applicable terms of this Statewide Contract. Prior approval of the customer is required for any subcontracted service of the Contract. Contractors are responsible for the satisfactory performance and adequate oversight of their subcontractors.

Construction Requirements

This contract may be used for construction, reconstruction, alteration, installation, demolition, maintenance or repair services and, if needed, associated materials. **All construction or construction related labor provided under this contract is limited to $50,000 or less per engagement.** Any services provided that would exceed $50,000 in labor costs must go out to a public bid.

Eligible Entities will be allowed to contract with any Contractor under Statewide Contract ITC71 for services for building or public works construction projects estimated to cost **less than $10,000** without the need to solicit multiple written price quotations when procuring these services, unless required by the Eligible Entity's internal procurement policies and requirements. Eligible Entities must use sound business practices which require a record that includes, at a minimum, the name and address of the person from whom the services were procured.

If using Statewide Contract ITC71 for building construction or public works projects estimated to cost **between $10,000 and $49,999** (this amount is capped for construction or construction-related labor only), **Eligible Entities are required to solicit a minimum of at least three (3) responses from ITC71 Contractors and MUST receive two (2) written responses from ITC71 Contractors**, provided that the contract shall be awarded to the responsible person offering to perform the contract at the lowest price quotation. If the project requires additional equipment/parts/materials the costs associated with such materials may exceed $50,000.

Tip: Buyers should request that vendors itemize their quotes so that the construction and/or construction-related services are isolated and easily identifiable. Only the labor costs are counted against the thresholds.

For purposes of construction procurement thresholds, **the act of pulling cables or wiring through existing conduits is not considered a construction activity**. The labor is however subject to prevailing wage law.

In instances where Statewide Contract ITC71 is used for construction or construction related labor in excess of $25,000, M.G.L c.149 s.29 **payment bonds** are required from the selected Contractor. It is the responsibility of the Eligible Entity to enforce this requirement when soliciting quotes. Eligible Entities may require additional performance and payment bonds from the Contractor, which would be detailed in the Statement of Work

The terms "Construction" and "constructed" are defined by M.G.L c. 149 s.27D. It is the responsibility of the Eligible Entity to consult their legal counsel for assistance determining whether installation work includes construction as defined by M.G.L. c.149 or M.G.L. c.30 s.39M. Information concerning specific construction requirements may be found in the Office of the Inspector General's Public Procurement Charts. Chapter 30B Procurement Assistance from the Office of the Inspector General is available at mass.gov/ig/procurement-assistance. Contact the 30B Hotline at 617-722-8838 or 30BHotline@mass.gov.

Supplier Diversity Requirements

When selecting contractors and placing orders, Executive departments shall utilize diverse and small businesses to the extent possible based on contract terms, SDO and departmental policies, laws, and regulations. Additionally, departments shall make a preference for contractors with higher SDP commitments and/or performance whenever such information is available (or is requested from contractors by the department) and the preference is feasible.

OSD provides up-to-date information on the availability of diverse and small businesses on statewide contracts through the Statewide Contract Index available on the COMMBUYS home page. See the "Programs (SDO and SBPP)" tab for current certification and small business status of contractors on this contract.

When soliciting quotes, the following requirements apply:

Expected annual value of the RFQ	RFQ process requirements
Less than or equal to $250,000/year	• **Notify at least two small businesses** capable of providing the product or service of the opportunity, if available. • Include SBPP contract language and place it prominently within the RFQ. • Evaluate bids received from, and award a contract to, an SBPP-participating small business that meets the department's best value criteria. • Award to a large business only if there is no SBPP participating business meeting departments' best value criteria. • Conduct a clarification/BAFO/negotiation before disqualifying an SBPP-participating business based on price or desirable criteria. • See the Best Value Evaluation of Responses to Small Procurements: A Guide for Strategic Sourcing Teams for additional guidance.
More than $250,000/year	• **Notify at least two diverse and/or small businesses** capable of providing the product or service of the opportunity, if available. • Make a preference for contractors with higher SDP commitments and/or performance whenever such information is available (or is requested from contractors by the department) and the preference is feasible. • **Note**: Departments may ask the prime Contractor for an additional SDP commitment specifically related to the Department's purchase or engagement. SDP spending for such a purchase or engagement must be reported by the Contractor using the SDP Reporting Form directly to the Department and may not be included in any other SDP reporting filed by the Contractor.

OSD provides up-to-date information on the availability of diverse and small businesses on statewide contracts through the Statewide Contract Index available on the COMMBUYS home page. See the "Programs (SDO and SBPP)" tab for current certification and small business status of contractors on this contract.

Pricing, Quote and Purchase Options

Pricing Options

- **Ceiling/Not-to-Exceed:** Contract discounts and other pricing published under the contract represents "ceiling" or "not-to-exceed" pricing, and may be further negotiated.

- **Category 1 – Catalog Sales**
  - Discount % off of MSRP or List price.
- **Category 2 – Security Systems Integration (Equipment and Related Services)**
  - Products: discount % off MSRP or List price for products.
  - Services: mark-up % over prevailing wage or hourly wage rates.
- **Category 3 – Security Systems Monitoring Services**
  - Service rates.
- **Category 4 – Locks, Locksmiths, Door Closures, and Related Hardware**
  - Products: discount % off MSRP or List price for products.
  - Services: mark-up % over prevailing wage or hourly wage rates.

Product/Service Pricing and Finding Vendor Price Files

Pricing is available for download from the Master Contract Record page.

Purchasing Options

The purchase options identified below are the only acceptable options that may be used on this contract:

- Purchases made through this contract will be direct, outright purchases

Category 2, 3 and 4 may include fee for service

Setting Up a COMMBUYS Account

COMMBUYS is the Commonwealth's electronic Market Center supporting online commerce between government purchasers and businesses. If you do not have one already, contact the COMMBUYS Help Desk to set up a COMMBUYS buyer account for your organization: (888)-627-8283 or OSDhelpdesk@mass.gov.

When contacting a vendor on statewide contract, always reference ITS71 to receive contract pricing.

Quick Search in COMMBUYS

Log into COMMBUYS, and use the Search box on the COMMBUYS header bar to locate items described on the MBPO or within the vendor catalog line items. Select Contract/Blanket or Catalog from the drop-down menu.

Obtaining Quotes

Contract users should always reference "ITC71" when contacting vendors to ensure they are receiving contract pricing. For non-construction related purchasing it is recommended that buyers solicit multiple quotes for purchases under this statewide contract. For projects involving construction or construction related labor, please review the Example Quoting Scenarios for Category 2 or 4.

For a full description of how to complete a quote in COMMBUYS visit the *Job Aids for Buyers* webpage, and select:

- The *COMMBUYS Purchase Orders* section, and choose *Request Quotes From Vendors on Statewide Contracts* job aid.

Instructions for MMARS Users

MMARS users must reference the MA number in the proper field in MMARS when placing orders with any contractor.

Emergency Services

Many statewide contracts are required to provide products or services in cases of statewide emergencies. ML - 801 CMR 21 defines emergency for procurement purposes. Visit the Emergency Response Supplies, Services and Equipment Contact Information for Statewide Contracts list for emergency services related to this contract.

Delivery/Returns

Delivery must be F.O.B. destination with no delivery or travel expenses paid by the Eligible Entity with the exception of deliveries to Dukes and Nantucket Counties. Contractor must deliver all purchases or initiate installation within thirty (30) business days after receipt of written order or at a time mutually agreed upon by the Eligible Entity.

Services and products/materials provided by Contractors must meet all federal, state, and local standards for quality and safety requirements. Services and products/materials not meeting standards will be deemed unacceptable and returned to a Contractor for credit at no charge to the Commonwealth.

Prevailing Wage Requirements

Services performed under Categories 2 and 4 may be subject to prevailing wage laws. Eligible Entities that utilize this contract will be considered the "awarding authority". Eligible Entities are required to request prevailing wage rate sheets at https://www.mass.gov/prevailing-wage-program (or by calling 617-626-6975) and provide these to the vendor. Vendors are responsible for complying with the Prevailing Wage law.

Category 4 – Locksmiths

Per the Massachusetts Department of Labor Standards, when covered by the prevailing wage, locksmith work falls under the carpenter rate.

Example Quoting Scenarios for Category 2 or 4

Example 1 – Construction or Construction Related Labor UNDER $10,000

You are an Eligible Entity soliciting quotes for a Category 2 or 4 project involving construction or construction related labor. Your quote for the construction or construction related labor costs are $8,500. Additional parts and materials will cost $12,000. The total estimated cost of this project will be $20,500.

STEP(S):

1. Select a vendor based on sound business practice/best value.

Example 2 – Construction or Construction Related Labor BETWEEN $10,000 and $50,000

You are an Eligible Entity soliciting quotes for a Category 2 or 4 project involving construction or construction related labor. Your quote for the construction or construction related labor costs are $35,000 and another $20,000 for pulling cables through existing conduits in your building. Additional parts and materials will cost $80,000. The total estimated cost of this project will be $135,000.

STEP(S):

1. **MANDATORY**: Request quotes from *at least three (3)* vendors on ITC71 within the same category.

2. **MANDATORY**: Receive *at least two (2) written responses* from vendors on ITC71 within the same category.
3. **MANDATORY**: Award project to the ITC71 vendor with the *lowest responsible response*.

Example 3 – Construction or Construction Related Labor GREATER THAN $50,000

You are an Eligible Entity soliciting quotes for a Category 2 or 4 project involving construction or construction related labor. Your quote for the construction or construction related labor costs are $75,000. Additional parts and materials will cost $150,000. The total estimated cost of this project will be $225,000.

STEP(S):

1. **MANDATORY**: Eligible Entity *must* go out to public bid and *cannot* use ITC71 due to labor costs being greater than $50,000.

How to Purchase From the Contract in COMMBUYS

Setting up a COMMBUYS Account

COMMBUYS is the Commonwealth's electronic Market Center supporting online commerce between government purchasers and businesses. If you do not have one already, contact the COMMBUYS Help Desk to set up a COMMBUYS buyer account for your organization: 888-627-8283 or COMMBUYS@mass.gov.

Directly purchase a non-fixed price item ($0 line item) through COMMBUYS

All vendor MBPO pages have a $0.00 line item for each category they are awarded. When placing an order in COMMBUYS a contract user needs to type in the total cost of the order and may add invoice/quote information as reference either by typing in the information or attaching as a file.

Solicit quotes and select and purchase quoted item in COMMBUYS

ITC71 has "Solicitation Enabled" category MBPO pages on COMMBUYS. This feature allows COMMBUYS users to obtain quotes from multiple vendors at once from the same category. The buyer would create a Release Requisition, and then convert it to a Bid. After approval by the buyer approving officer, the bid is then sent to selected vendors to request quotes.

For more information on how to complete this purchase in COMMBUYS, visit the *Job Aids for Buyers* webpage.

Additional Information/FAQs

Banning of Dahua and Hikvision

In response to the ban enacted by H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019, Section 889 on Hangzhou Hikvision Digital Technology Company and Dahua Technology Company (or any subsidiary or affiliate of such entities) products from both manufacturers are forbidden on ITC71.

Proprietary Product Exclusion

Purchase of any software package for any security purpose that is unique to one Contractor or proprietary in any manner is strictly prohibited. All included hardware and software provided by Contractors must be serviceable by companies other than the Contractor and shall be designed for service and maintenance by others. It is the goal of the

Commonwealth to procure off the shelf platforms that can be serviced by multiple Contractors at the option of the Commonwealth. Eligible Entities may request program codes specific to each system as well as the platform on which the codes reside on.

Negotiation

Eligible Entities have the right to negotiate pricing or other aspects of purchases within the scope of the contract and are encouraged to do so.

Pre-Installation

It is the Vendor's responsibility, prior to delivery, to survey and review the particular installation location to ensure the existing proposed location will meet the manufacturer's established installation criteria. Should the proposed installation location not meet established installation criteria, the Vendor and the Eligible Entity will attempt to locate an alternate mutually agreeable location for the equipment at the particular site.

Vendors not familiar with any location are strongly advised to personally view those locations prior to delivery. A lack of familiarity with an installation location will in no way relieve a vendor from its responsibility to fulfill its contractual obligations.

Compliance with Regulatory Requirements

Vendor must maintain full compliance with all Regulatory Licensure Boards' (State Board of Electrical Examiners, Department of Public Safety) licensing requirements for all work.

Post-Installation

Vendor must be responsible for all installation of equipment and/or supplies and removal of all package material from the premises in coordination with the Eligible Entities instructions. For off-site monitoring services, Vendor must ensure there are systems current to meet the needs of the Commonwealth and remain current against intrusive/invasive systems that could compromise the installed system(s).

Anticipated Service Disruption

Vendor must coordinate with the Eligible Entity for any anticipated service disruption. If anticipated disruption is scheduled the Vendor must provide a minimum of 24 hours' notice to the Eligible Entity.

Training and Training Materials

Vendors must provide significant training to designated personnel within the Eligible Entity during the final system testing and start-up phase of a project. The vendor and Eligible Entity shall mutually agree on the duration as well as the location and schedule of the training. Training materials include, but are not limited to books, handouts, software, or customized training videos will be provided by the vendor and will be given to the Eligible Entity at no additional cost, as agreed upon by the parties.

Software Licenses

Where applicable, the cost of software licenses should be included in the Service Maintenance Agreement. Eligible Entities may also purchase software licenses separate from any Service Maintenance Agreements.

Warranties

Vendors must provide a standard warranty for all equipment of at least 1 year in length. Eligible Entities may purchase extended warranties with vendors at negotiated pricing. Please review the ITC71 price file on COMMBUYS for information regarding the availability of extended warranties. Vendor must affix a label or decal to the control device for any equipment at the time of installation showing warranty period by dates, and the name, address, and telephone number of the OEM or Reseller responsible for warranty service of the equipment. A successful installation is constituted by the product, equipment or system being fully capable of functioning to its fullest capacity and according to its design and is unencumbered by flaws resulting from poor installation. System Acceptance (final sign-off) will be provided by the user entity acknowledging final acceptance of a successful installation. System Acceptance cannot be unreasonably withheld by any entity, the contract manager or the project manager.

No pre-payments

Vendor may not request any form of pre-payments by the Eligible Entity before the service is rendered. For special projects implemented in phases, by mutual agreement of the Eligible Entity and the Vendor, invoices must be issued after each phase is completed to the Eligible Entity's satisfaction.

No Minimum Charge

Contractors are paid only for hours worked on location. Labor charges begin at job location and end at job location. Eligible Entity will not pay for any additional labor charges away from job location.

No Additional Fees and Surcharges

Contractors are not allowed to charge additional fees or surcharges with the exception of deliveries to Dukes and Nantucket Counties. This includes, but is not limited to, charges for permits, set-up, cleaning, freight, shipping, quotes, travel, transportation, delivery, commuting, fuel, energy, insurances, meals, lodging, and any other fee.

Statement of Work Example

Eligible Entities should provide a clear Statement of Work to the vendors at the time of the request for quote. The following are some elements to consider including in a statement of work:

Important Elements of the Statement of Work:

- Reference to the Statewide Contract ITC71
- Prevailing wage sheets, as applicable to the job
- Work schedules and performance dates
    - Release Date of the Request for Quote
    - Walkthrough requirements, if required
    - Response Date of Request for Quote
    - Date of Vendor Selection
- Responsibilities of the Vendor
    - Agrees to fulfill all provisions of the ITC71 statewide contract
    - Responsible for complete design, measurements, and drawings
    - Delivery, installation, testing, training, design and start up
    - Replace, modify, or upgrade existing hardware as necessary

    - Include the cost of any software licenses in bid
- Whether sub-contractors will be allowed
- Eligible Entity Reserves right to negotiate and modify requirements with awarded Vendor
- Submittal Requirements
    - Narrative – how proposer will complete scope of work
    - Estimated timeline from release of purchase order to system live
    - Drawing Requirements
- Service/Maintenance Agreements
    - Response time guarantees desired
- Up time guarantee

Strategic Sourcing Team Members

- Amanda Ferdinand, OSD
- Arthur Venier, DOC
- Cindy Heywood, DOC
- Eric Josephson, City of Cambridge
- Jeff Quick, DOC
- Kristin Cafarelli, DOE
- Mark Gerrity, Trial Courts
- Nancy Fitzgerald, DFS
- Roger Gauthier, DPH
- Sergio DeMango, Town of Lexington
- Tim Kennedy, OSD

Vendor List and Information*

Vendor Name *(SDO**)*	Contact Person	Phone #	Email	Categories	Regions	PPD (%-days)	SDP Commitment Percentage	SDO Certification Type
Master Contract Record***	Amanda Ferdinand	617-720-3166	Amanda.Ferdinand@mass.gov					
Category 1 Catalog Sales****								
Category 2 Integration****								
Category 3 Monitoring****								
A W Gifford Inc.	Denice Outhuse	413-732-8951	denice@giffordlock.com	4	1	2%-10	2%	
Access Control Systems Inc.	Tim Kirk	603-248-9820	sales@a-c-s.biz	1 and 2	All	1%-10; 0.5%-15; 0.1%-20	1%	
Advanced Alarm Systems Inc.	Kevin C. Fitzpatrick	508-675-1937	kevin@80044alarm.com	2 and 3	2, 4, and 5	2%-10; 1.5%-15; 1%-20	5%	
ADT COMMERCIAL LLC	James McDonald	774-218-5140	jamesmcdonald@adt.com	All	All	2%-15	6%	
Alarm New England *(SSH3, Inc. dba Sonitrol New England)*	Ana Goncalves	860-616-7544	ana.goncalves@alarmnewengland.com	2 and 3	All	3%-10; 2%-15; 0.25%-20	15%	
American Alarm & Communications Inc.	Barry Chisholm	781-859-2051	bchisholm@americanalarm.com	2 and 3	All	1%-30	1%	
American Service Company	Sarah Kelly	617-471-5953	skelly@americanservicecompany.com	1, 2, and 3	2, 3, 4, and 5	2%-30	1%	
Autoclear LLC	Jon Martin	973-369-5569	jonm@autoclear.com	1 and 2	All	1%-10	1%	
Ayacht Technology Solutions, LLC	Beverley A. Denio	978-558-0166	bdenio@ayacht.com	2	All	1%-10; 0.5%-15; 0.25%-20	3%	
Barrett Security and Surveillance	Rick E. Barrett Jr.	617-268-8078	brrttrod@aol.com	1 and 2	All	10%-10; 8%-15; 6%-20; 4%-30	10%	
BCM Controls Corporation	Steve Feinberg	781-897-5160	feinbergs@bcmcontrols.com	2 and 3	All	3%-15; 2%-20; 1%-30	5%	
BeSafe Technologies Inc.	Michael O'Keefe	508-815-3540	mokeefe@besafe.net	2	All	5%-10; 4%-15; 3%-20; 2%-30	1%	
Boston Electric and Telephone Corp	Hiram Falfan	617-828-9608	hiram@betcorp.com	1 and 2	2, 3, 4, and 5	2%-15	2%	
BSA Security Integrators *(Bay State Alarm Security, Inc. dba BSA Security Integrator)* ***SDVOBE***	TJ Murphy	508-485-1174 x113	tj@bsasi.com	All	All	2%-10; 1.5%-15; 1%-20	3%	
CC-Teknologies Inc.	Robert Armstrong	781-767-7640	rob@cc-tek.net	All	All	3%-10; 2%-15; 1%-20	3%	

Vendor Name *(SDO**)*	Contact Person	Phone #	Email	Categories	Regions	PPD (%-days)	SDP Commitment Percentage	SDO Certification Type
Ceia USA Ltd.	Jep Poole	440-836-2889	jpoole@ceia-usa.com	1	All	1%-15	6%	
Collins Electric	Mike Angelica	413-598-1024	mangelica@ce1906.com	2	1 and 2	1.5%-10; 1%-20	10%	
Comm-Tract Corp	Rod Jenks	781-890-5070 x6927	rjenks@comm-tract.com	2	All	4%-10; 3%-15; 2%-20; 1%-30	5%	
Convergint Technologies (DG investment Intermediate Holdings 2)	Helio Leal	617-831-5558	helio.leal@convergint.com	1, 2, and 3	All	2%-30	1%	
Craftmaster Hardware	Kevin Driscoll	508-661-9632	kdriscoll@craftmasterhardware.com	1	All	2%-10; 1%-15	6%	
CSDNET *(Networked Educational Technologies Ltd. dba CSDNET)*	Fred Zapollo	631-924-7474	fred.zappolo@csdnet.net	1 and 2	All	3%-10; 2%-15; 1%-20	10%	
CSY Technologies	Richard Netinho	774-202-7258	rnetinho@csytech.com	1 and 2	All	3%-10; 2%-15; 1%-20	5%	
Custom Computer Specialists, Inc.	Suzanne McLaughlin	401-775-1286	smclaughlin@customonline.com	2	All	1%-30	1%	
D.H. Pace Company, Inc. dba. Pasek Corporation	David Alessandrini	617-269-7110 x112	dalessandrini@pasek.com	All	All	2%-15	1%	
Dugmore & Duncan, Inc.	Skip Reid	781-927-2118	skip@dugmore.com	1 and 4	All	2%-10	1%	
ECI Systems	Kellie Porter	603-458-6506	kellie.porter@ecintegrated.com	2	All	1%-20	2.50%	
Electronic Security and Control Systems Inc.	Ben Jacobellis	781-271-0830	benny3@escsinc.com	2, 3, and 4	All	2%-10; 1%-15; 0.5%-30	1%	WBE
ENE Systems, Inc.	John Doherty	781-828-6770	jdoherty@enesystems.com	All	All	1%-30	2%	
ePlus Technology	Steve Low	781-615-1314	slow@eplus.com	1	All	2%-10; 1%-30	2%	
FRANK H PERRY III dba. White Hawk Alarm & Security	Frank Perry	978-597-8800	whitehawkalarm@gmail.com	All	1, 2, 3, and 4	3%-10; 2%-30	1%	
FS Systems Inc.	Cheryle O Sullivan	781-754-7310	cosullivan@fssystemsinc.com	1, 2, and 4	All	3%-10; 2.5%-15; 2%-20; 1%-30	10%	
Galaxy Integrated Technologies, Inc.	John Gulezian	617-202-6388	johng@galaxyintegrated.com	1, 2, and 4	All	3%-10; 2%-15; 1%-20	10%	
Graybar Electric Company Inc.	John Ryan	781-205-8719	john.ryan1@graybar.com	1	All	1%-10	1%	
Hayden Safe & Lock Co., Inc.	John Whitmarsh	978-265-5837	john@haydenlock.com	1 and 4	3 and 4	5%-10; 4%-15; 3%-20; 2%-30	5%	
HEI Security	Brian Nelson	801-784-4163	brian.nelson@heisecurity.com	1, 2, and 4	1, 2, and 3	1%-10	10%	
Industrial Video & Control Co. LLC	Dipak Sagar	617-467-3059 x122	dsagar@ivcco.com	1	All	2%-10; 1%-15	5%	

Vendor Name *(SDO**)*	Contact Person	Phone #	Email	Categories	Regions	PPD (%-days)	SDP Commitment Percentage	SDO Certification Type
Ironman Inc.	James Hatch	508-594-8038	commbuys@ironmans.net	1	All	2%-10; 1.5%-15; 1%-20; 0.5%-30	5%	
Tyco Fire & Security Management Inc dba Johnson Controls Security Solutions	Alison Jaclyn	781-953-1883	alison.jaclyn.scali@jci.com	1, 2, and 3	All	2%-10; 1%-15	10%	
K & M Communications Corp.	Melanie Correia	508-857-2011 x106	accounting@kandmcommunications.com	2, 3, and 4	All	2%-15; 1%-30	10%	VBE
Kamco Supply Corp.	Brian Messina	781-897-7221	bmessina@kamcoboston.com	4	2, 3, 4, and 5	2%-10; 1%-20	2%	
KNE Corporation	Victor Conklin	781-762-8344	victor@knecorp.com	4	All	2%-10	1%	
LAN-TEL Communications, Inc.	Dennis Drain	781-352-4134	ddrain@lan-tel.com	2 and 3	All	3%-10; 2.5%-15; 2%-20; 1%-30	5%	
McDonald Electrical Corporation	Nick Flynn	339-205-2227	nflynn@mcdonaldcorp.com	1, 2, and 3	All	2%-20; 1%-30	10%	
Minuteman Security Technologies	John Mendonca	978-783-0018	johnm@minutemanst.com	2, 3, and 4	All	2%-10; 1%-15	5%	
New Era Technology NE (Future Technologies Group LLC)	Kate Waldron	617-502-1248	Kate.Waldron@NewEraTech.com	2 and 3	All	3%-15; 1%-20	7%	
NOREL Service Co. Inc.	George Aguiar	781-768-5500 x111	gaguiar@norelservice.com	1, 2, and 3	2, 3, 4, and 5	2.5%-10; 1.5%-15; 1%-20	10%	VBE
Ockers Company	Jason Houser	508-586-4642	jasonh@ockers.com	1 and 2	All	3%-10; 2%-20; 1%-30	3%	
Plastic Card Systems, Inc.	Donald Axline	508-351-6210 x102	daxline@plasticard.net	1 and 2	All	2%-10; 1%-15	10%	WBE
Presidio Networked Solutions, LLC.	Drew Koellmer	781-638-2379	dkoellmer@presidio.com	1 and 2	All	1%-10	2%	
Schneider Electric Buildings Americas, Inc.	Thomas Sullivan	978-994-8378	Thomas.sullivan@se.com	2	2, 3, 4, and 5	2%-10	10%	
Surveillance Specialties, Ltd. dba Allied Universal Technology Services	Michael Devita, III	978-253-5023	michael.devita3@aus.com	1, 2, and 3	2, 3, 4, and 5	1.75%-10; 1.5%-15; 1.25%-20	5%	
Security101 *(Advanced Security Integration dba Security101)*	Main Office	1-800-991-4170	support@security101ne.com	All	All	1%-10	15%	
Setronics Corp.	Brian LaCroix	978-671-5450	blacroix@setronics.com	2, 3, and 4	All	1%-10	10%	
SIGNET Electronic Systems, Inc.	Gregory S. Hussey	781-871-5888	greg.hussey@signetgroup.net	2	All	2.5%-10; 1.5%-15; 1%-20	3%	

Vendor Name *(SDO**)*	Contact Person	Phone #	Email	Categories	Regions	PPD (%-days)	SDP Commitment Percentage	SDO Certification Type
Sonet Electrical Systems LLC	Tom Cavanaugh	617-242-6569 x222	tcavanaugh@sonetelectrical.com	2	3, 4, and 5	2%-10; 1.5%-15; 1%-20	1%	
Siemens Industry Inc.	Jonathan Hipsh	857-205-7598	jonathan.hipsh@siemens.com	2 and 3	All	1%-30	5%	
Spectrum Integrated Technologies *(J&M Brown Company, Inc. dba Spectrum Integrated Technologies)*	Steven Feldman	617-522-8800	sfeldman@spectrumit.com	2	All	1%-10; 0.5%-15; 0.25%-20	5%	
Stanley Convergent Security Solutions, Inc.	Larry Movessian	781-460-4528	larry.movsessian@sbdinc.com	All	All	2%-10; 1%-30	5%	
State Electric Corp.	Jeff Flynn	978-341-5181	jflynn@stateelectriccorp.com	1 and 2	All	2.25%-10; 1.5%-15; 1.25%-20; 1%-30	10%	
Stone & Berg Company Inc.	Jeremy Conroy	978-973-4711	j_conroy@mac.com	1	All	2%-20	2%	WBE
Sullivan and McLaughlin	Maeve Comer Marshall Jones	617-474-0500 Ext. 275 617-593-0985	mcomer@sullymac.com mjones@sullymac.com	2	All	5%-10; 4%-15; 3%-20; 2%-30	10%	
Unified Networking Solutions	Brian McDonald	508-203-7162	bmcdonald@unifieditsupport.com	1 and 2	All	4%-10; 3%-15; 2%-20; 1%-30	5%	
Utility Communications Inc.	Barbara Gengarelly	203-287-1306	barbarag@utilitycommunications.com	1	All	2%-10; 1%-15; 0.5%-20; 0.25%-30	3%	
Valley Communications Systems, Inc.	Jim Page	413-386-6221	jimp@valleycommunications.com	2	All	1.5%-10; 1%-15	5%	
Viscom Systems Inc.	Bill Clements	617-864-3676	bill.c@viscomsystems.com	1 and 2	2, 3, 4, and 5	2.5%-10; 1.5%-15; 1%-20	10%	
Wayne Alarm Systems Inc.	Paul Verruto	781-595-0000 x426	pverruto@waynealarm.com	2 and 3	2, 3, 4, and 5	2%-15; 1%-30	7%	
Whalley Computer Associates Inc.	Paul Whalley	413-569-4200	wcabiz@wca.com	2	All	1%-10	10%	

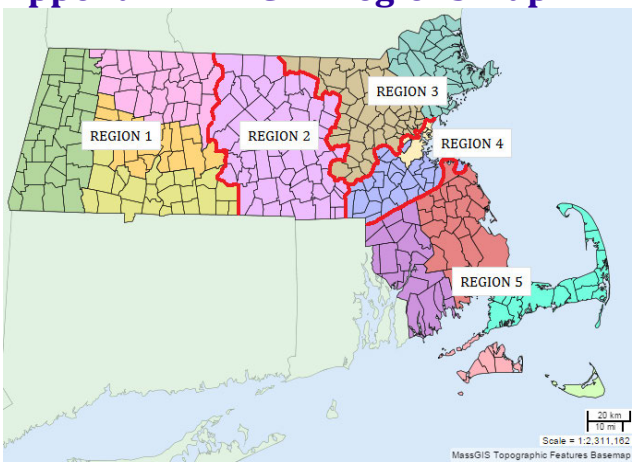
* COMMBUYS is the official system of record for vendor contact information.

** SDO – Supplier Diversity Office. Vendors with SDO certifications have their certification listed with their vendor name.

*** The Master Contract Record page holds additional information such as the ITC71 RFR and ITC71 Master Price File.

**** Category pages in COMMBUYS are solicitation enabled to allow for convenient quoting in COMMBUYS.

Appendix A: ITC71 Regions Map



Region 1: • Berkshire County • Franklin County • Hampden County • Hampshire County	**Region 4:** • Norfolk County • Suffolk County
Region 2: • Worcester County	**Region 5:** • Barnstable County • Bristol County • Dukes County • Nantucket County • Plymouth County
Region 3: • Essex County • Middlesex County	

Appendix B: Contract Categories

Category 1: Catalog Sales

This category is only for catalog sales for security equipment and supplies that is within the scope of this contract.

Category 2: Security Systems Integration (Equipment and Related Services)

This category is to provide security integration services; specifically the Contractor must be able to provide equipment, systems, supplies, installation, design services, training, service and maintenance, and technical support for all equipment and related services. This includes, but is not limited to: configuration and integration of security, camera, access control, or ID systems and supplies; lobby turnstiles; vehicle access barriers; command centers; detection systems (including x-ray machines, metal detectors, full-body scanners, explosives, narcotics, vehicle-borne, environmental, buried cable, fence, or infrared detection systems); racks, housings, security consoles, mounts, stand-alone computers, secured data storage (local and/or cloud), encrypted data transmission (wired, wireless, and/or cloud-based) and the ability to track encrypted data transmissions; and furniture/fixtures when designed or purchased for use in a security application.

Category 3: Security Systems Monitoring Services

This category is to provide security systems monitoring services in following types of locations: facilities (buildings, garages, tunnels, etc.), campuses (groups of buildings, that may include fencing and gates, etc.), and residential group homes. Category 3 is for system monitoring services ONLY. Contractors wishing to provide both monitoring and installation services must submit proposals under both Category 2 and Category 3.

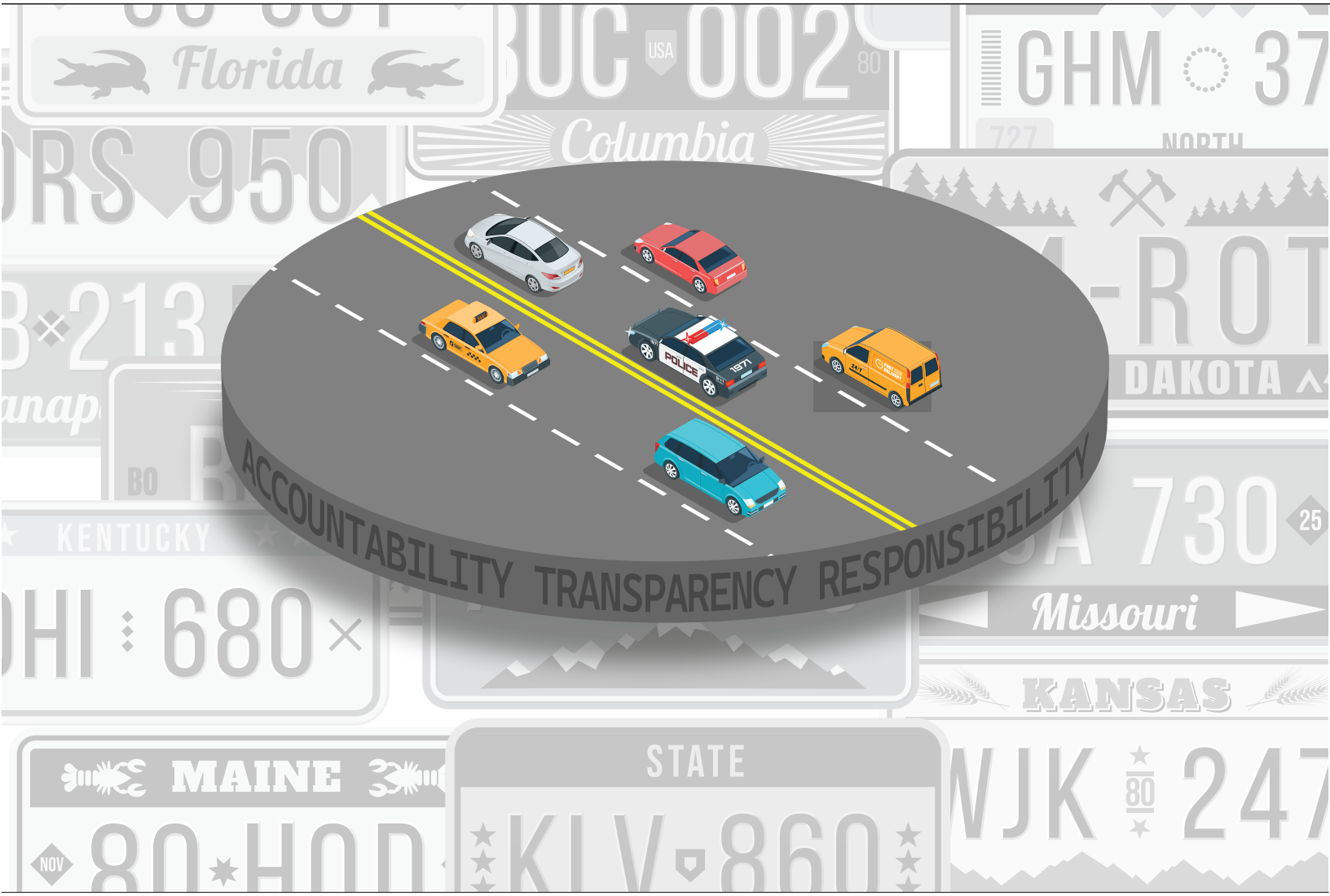
Category 4: Locks, Locksmiths, Door Closures, and Related Hardware

This category is to provide full-service installation, maintenance, and catalog sales of locks, accessories, and related equipment. This includes, but is not limited to padlocks, locks, keys, mortis locks, lock cylinders, auxiliary, deadbolt, door closures, key making machines, supplies and repair parts, handicap door openers, panic bars, hasps and hasp locks, institutional locks and door systems (paracentric locks, high security mogul locks, sliding door operators-institutional) and accessories, safes, and locksmith tools or security supplies.

MAJOR CITIES CHIEFS ASSOCIATION

Automated License Plate Reader Technology in Law Enforcement

RECOMMENDATIONS AND CONSIDERATIONS



PRESENTED BY MCCA ALPR WORKING GROUP

Table of Contents

Introduction — I
Executive Summary — II
Key Recommendations — III
Methodology of Product — IV
What is an Automated License Plate Reader? — 1
- ALPR Hardware and Software
- Types of ALPR
- The ALPR Detection Record
- Hotlist Sources
- Tactical vs. Investigative Uses
- Business/Private Use

Program Design and Development — 3
- Policy Development
- Training Considerations
- Deployment Strategies

Procurement — 7
- Vendor and Product Assessment
- Technical Challenges
- Procurement Ethics

Program Management and Oversight — 9
- Access and Appropriate Use
- Data Sharing
- Auditing, Data Collection, and Reporting

Data Stewardship — 13
- Data Roles and Responsibilities
- Data Security
- ALPR Reader Device Integrity

ALPR Operations Infographic — 15
ALPR Synergy with Other Law Enforcement Technologies — 16
- Beyond ALPR: AI-Enhanced Vehicle Detection

Case Law Related to ALPR — 17
- Privacy Expectations on Public Roadways
- Is ALPR Persistent Tracking?
- License Plates & Personally Identifiable Information (PII)
- Data Collection & Sharing
- ALPR Hits & Degrees of Intrusion

Conclusion — 21
Acknowledgments — 22
Definitions — 23
Appendix A – Success Stories — 24
Appendix B – Myths and Misconceptions — 26
Appendix C – State-Level Laws and Regulations — 28
Appendix D – CJIS Security Policy — 31
Appendix E – ALPR Audit and Transparency Report Template — 33

2618

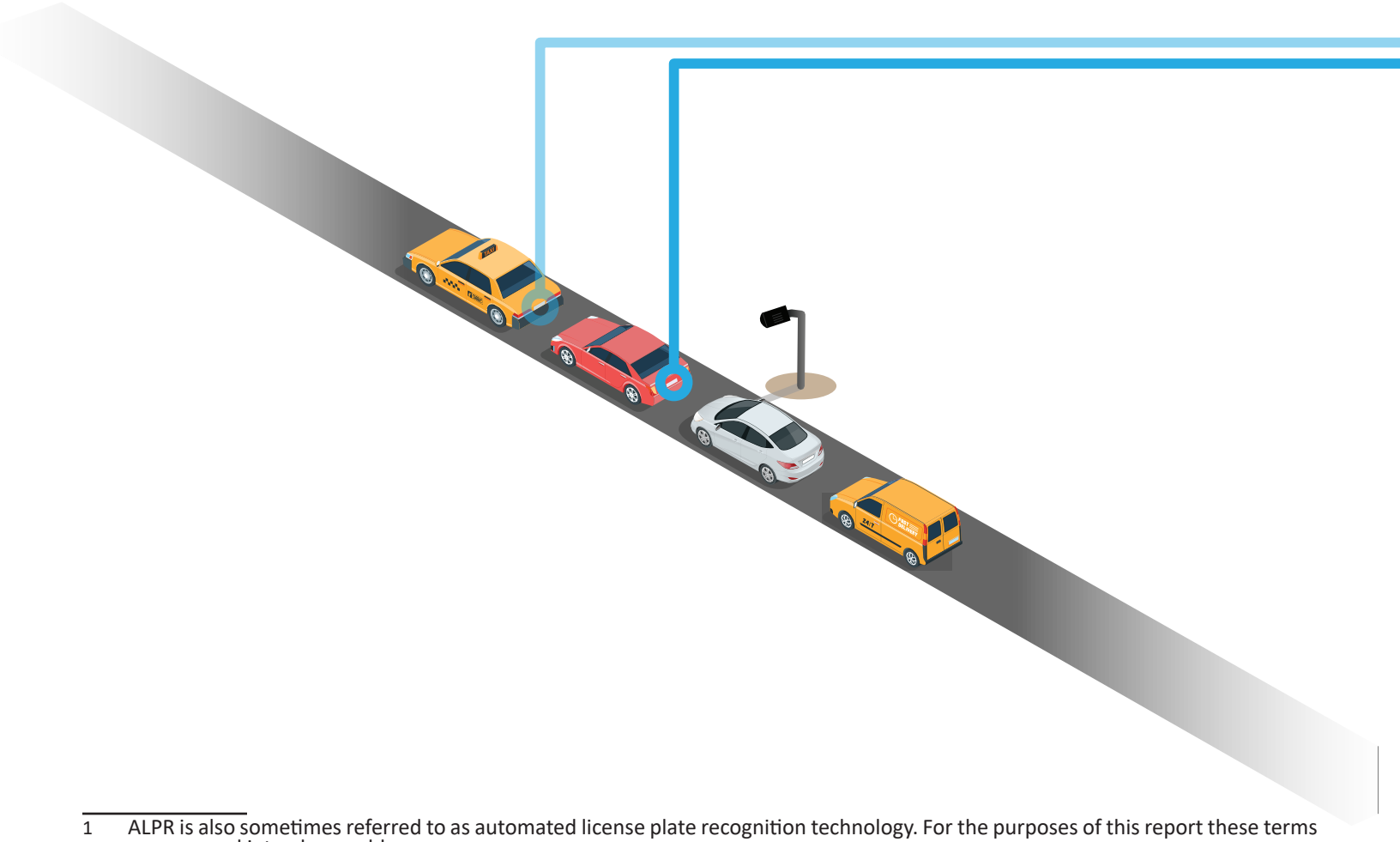
Introduction

Modern-day law enforcement relies on advanced technologies to enhance investigative capabilities. One example of these technologies is automated license plate reader (ALPR).[1] ALPR has been used for decades by law enforcement agencies throughout the United States, Canada, and across the globe to help generate leads and close cases. Law enforcement agencies that utilize ALPR continuously report that the technology is a critical tool that helps advance their efforts to fulfill law enforcement's ultimate mission of keeping our communities safe.

ALPR is a proven technology, but all law enforcement tools must be used ethically and appropriately. This product is designed to assist law enforcement agencies with developing and maintaining an ALPR program that respects citizens' Constitutional rights and privacy while maintaining ALPR's effectiveness as a tool to address crime.

In October 2022, the Major Cities Chiefs Association (MCCA) established an ALPR Working Group composed of trusted technology partners, law enforcement agency stakeholders, and subject matter experts in the ALPR field to achieve this goal. The Working Group has created a set of best practices related to procurement, development, operation, data collection and reporting, and other elements instrumental in creating a well-balanced ALPR program. Like any other technology, ALPR will continue to evolve.

The product is a true public-private partnership, and the framework outlined in it will help law enforcement agencies seeking to utilize ALPR achieve the highest possible standards. However, it is essential to remember that every community is different, and what works in one community may not work in another. Therefore, while the Working Group's recommendations provide a strong foundation, agencies are encouraged to tailor them to meet the specific needs of their community as they develop, implement, and manage their ALPR program.



1 ALPR is also sometimes referred to as automated license plate recognition technology. For the purposes of this report these terms are used interchangeably.

2619

Executive Summary

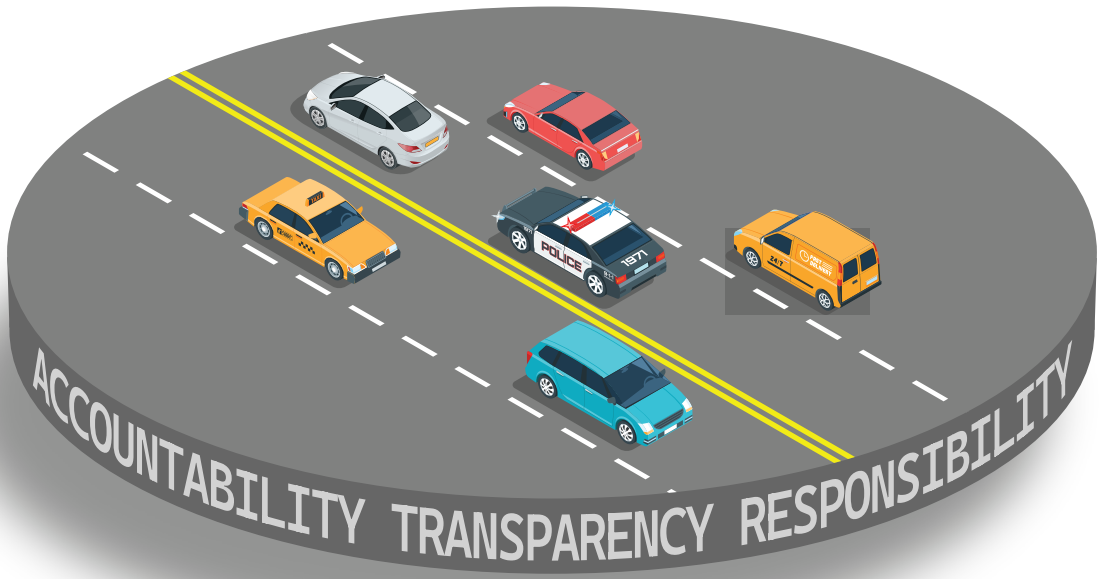
In October 2022, the Major Cities Chiefs Association (MCCA) launched an ALPR Working Group composed of trusted technology partners, law enforcement agency stakeholders, and subject matter experts. The Working Group has developed a product that is designed to provide MCCA members and other law enforcement agencies with guidance on developing, deploying, and responsibly using ALPR technology. ALPR technology has proven to be a powerful tool to combat criminal activity, generate actionable investigative leads, and help close cases faster.

This product directly addresses the most critical aspects of ALPR technology, which can be subdivided into three main categories: accountability, responsbility, and transparency. The product outlines suggestions on ALPR program design, policy development, training considerations, and deployment strategies. The product also covers ALPR procurement. Finally, it addresses the ongoing management and oversight of the technology and provides an overview of relevant case law. While these suggestions and recommendations address the most critical aspects of ALPR, they leave sufficient room for agencies to develop programs that meet their specific needs.

Stakeholders concerned about ALPR typically focus on disparity of impact, infringement of privacy, and the effects on individual rights. However, the Working Group strongly believes these concerns can be sufficiently addressed and mitigated through thoughtful policy design, effective management, and proper oversight. Furthermore, it is important to note that recent case law differentiates the capabilities ALPR provides from those of other law enforcement technologies.

The guidance outlined in this product serves as a template for building and operating an ALPR program that is both effective in its use and responsible in its nature. By implementing the Working Group's suggestions and recommendations, law enforcement agencies can ensure their ALPR programs are helping to keep communities safe while protecting citizens' privacy, civil liberties, and Constitutional rights. In addition, this can help increase public trust and build support for using ALPR technology.

Finally, like all technology, ALPR will continue to change and evolve. For this reason, this product should be considered a living document rather than a finalized template for developing and implementing a balanced and responsible ALPR program. As the conversation surrounding ALPR progresses, so will the recommendations and suggestions included in this product.



2620

Key Recommendations

The following key recommendations serve to highlight the MCCA ALPR Working Group's most essential recommendations and considerations. They have been grouped by their applicability to three foundational principles regarding the deployment of advanced technologies in law enforcement.

ACCOUNTABILITY

- Agencies should develop a training program that establishes accountability guidelines, procedures for responsible use, and emphasizes transparency. The use of ALPR technology should be limited to trained personnel.
- The use of ALPR technology should be limited to criminal investigations or to address an articulable public safety concern.
- The procedures for the use of ALPR technology should emphasize the need to confirm the accuracy of the information presented prior to taking enforcement action.
- Careful consideration should be given to the data retention policies implemented by the agency. Data retention time frames should be developed by balancing community needs, benefits, and concerns.
- Audits of ALPR programs should be conducted regularly. Audits should monitor user activity to ensure appropriate use in accordance with established policies.

RESPONSIBILITY

- Sharing ALPR data among law enforcement agencies can enhance the effectiveness of ALPR deployments. A clear policy should be established prior to enabling data sharing to address data usage and deconfliction requirements.
- Deployment strategies should be reviewed regularly and evaluated to ensure the ALPR program and technology continues to operate within the established objectives and policies.
- Law enforcement agencies seeking to procure ALPR technology should consult with other agencies that have deployed ALPR during program development.
- Prior to the deployment of ALPR technology, agencies should assess existing technological deployments and consider how they can complement or enhance their specific program strategy.
- Law enforcement agencies must implement strict cybersecurity protections to prevent unauthorized access of ALPR data.

TRANSPARENCY

- Deployment plans should be informed by analyzing crime data, patterns, and trends to ensure the technology is deployed in an equitable and responsible manner.
- Agencies should consult with their local public works and other relevant stakeholders to ensure the ALPR deployment plan meets all permitting, legal, and other requirements.
- Comprehensive data collection and reporting will help maximize the benefits of ALPR technology by increasing transparency and empowering agencies to determine its impact on crime and public safety.

2621

Methodology of Product

This product represents the comprehensive collection of the MCCA ALPR Working Group's recommendations and considerations regarding law enforcement's use of ALPR technology. The value of ALPR as a crime-fighting tool is well established. However, an effective program must include certain elements to ensure the technology is being used effectively and in a manner that maintains the trust and support of the community. This document will provide law enforcement agencies with a framework to develop, implement, and manage an ALPR program that is based on responsible use, helps keep the community safe, and respects privacy, civil rights, and civil liberties.

The MCCA ALPR Working Group includes technology vendors from various backgrounds, a diverse group of law enforcement professionals, and ALPR subject matter experts. In addition, the Working Group conducted in-depth research on ALPR technology from numerous perspectives. Finally, the Working Group leveraged the expertise of the individual participants to develop its recommendations and suggested best practices.

The information and data used to support the findings of this product include material provided by MCCA member agencies and technology vendors. The Working Group also reviewed products produced by other stakeholders on ALPR and the use of technology in policing more generally. Finally, the Working Group conducted regular internal discussions to finalize the recommendations and suggested best practices.

This product's outline and overarching topics were created collaboratively with input from all Working Group participants. Each participant was responsible for drafting a section of the report, and those drafts were circulated to the entire Working Group for review. All Working Group members approved the final product.

The final product represents the MCCA ALPR Working Group's findings, recommendations, and suggested best practices. These will help law enforcement agencies create, manage, and operate an effective and responsible ALPR program.

2622

What is an Automated License Plate Reader?

ALPR, called Automated Number Plate Recognition (ANPR) in Europe, was invented in 1976 by the Police Scientific Development Branch to combat terrorism in the United Kingdom. While seen as a valuable tool, the associated cost and requisite experience stagnated the deployment and advancement of the technology until the first ALPR cameras were installed at the Dartford Tunnel and A1 Road in 1981. The Dartford Tunnel cameras resulted in ALPR's first arrest for a stolen vehicle. This slowly led to more widespread use of the technology, including as part of the "ring of steel" created around London in the early 1990s to protect against the Irish Republican Army (IRA) bombing campaigns. Later, ALPR technology was also deployed as part of another initiative entitled "Project Laser," which sought to "target criminals through their use of roads."[1]

The success of the "ring of steel" and "Project Laser" prompted the Police Standards Unit to create the National ANPR Data Centre (NADC) in 1997. The NADC allowed for the nationwide sharing of ALPR data across the United Kingdom and the Back Office Facility (BOF), the database where ALPR data was stored and analyzed. ALPR technology took off from here. Law enforcement first used ALPR to help solve a murder case in 2005, and by 2007, nearly half of all law enforcement agencies in the UK were using ALPR technology. American law enforcement agencies followed their British counterparts closely and started using ALPR in 1998.[2]

ALPR Hardware and Software

While the technology has advanced over the years, the main components of those early ALPR deployments and today's systems remain the same. At its core, an ALPR program consists of the camera hardware and the software used to store and analyze the generated data and alert the users when a detection of interest is made. In most cases, ALPR hardware consists of a camera, processor, power supply, and data transfer hardware. In addition, ALPR cameras are typically optimized in various ways to operate in a wide range of real-world conditions (low light, inclement weather, motion detection, etc.).

Once the camera captures the image, ALPR systems use software to read the license plate. Some systems process the image at the camera level. Other systems transfer (usually via a cellular network, but it may occur through other means) data from the camera to a dedicated ALPR-system computer for processing. The image is analyzed through Optical Character Recognition (OCR) software as part of the processing. OCR recognizes alpha-numeric numbers and letters, thereby allowing the ALPR system to successfully recognize and interpret any letters or numbers observed in the image captured by the camera.

Types of ALPR

Law enforcement uses various types of ALPR technology, including fixed, mobile, portable, and mobile applications. Below is a description of each kind of ALPR system:

- **Fixed ALPR** cameras are typically permanently mounted to infrastructure such as traffic signals, bridges, and light poles.
- **Mobile ALPR** cameras are typically mounted on vehicles. These cameras may be overtly or covertly deployed depending on the needs of the law enforcement agency.
- **Portable ALPR** cameras include mobile camera trailers which can be transported and deployed based on the law enforcement agency's operational needs.
- **Mobile Applications** leverage features built into cellular devices to create ALPR detections.

1 David J. Roberts and Meghann Casanova, Automated License Plate Recognition (ALPR) Systems: Policy and Operational Guidance for Law Enforcement, National Institute of Justice, U.S. Department of Justice, 2012. https://www.ojp.gov/pdffiles1/nij/grants/239605.pdf

2 B.A. Reaves, Local police departments, 2013: Equipment and Technology. Bureau of Justice Statistics, U.S. Department of Justice, July 2015. https://bjs.ojp.gov/library/publications/local-police-departments-2013-equipment-and-technology

2623

The ALPR Detection Record

An ALPR record is generated when a vehicle license plate is detected, imaged, and processed to create a record. An individual ALPR record (or 'plate read') is generally composed of the following:

- An image of the license plate, which is a 'cropped' digital image of the license plate captured by the camera.
- The geo-location where the plate detection occurred, which can be determined from the GPS coordinates of a mobile reader or inferred from the location where fixed readers are placed.
- The time and date when the license plate detection occurred.
- The translated information from the plate, which is the alpha-numeric plate number and the issuing organization, typically a state. This translation can be accomplished by OCR or artificial intelligence.

In addition, an ALPR record may contain the following:

- A collateral image of the vehicle for which the ALPR read occurred.
- Metadata associated with the camera that identifies the camera unit, image settings, and other specific attributes.

Hotlist Sources

ALPR systems used by law enforcement can alert on detections of wanted vehicles. Two primary methods exist for creating a wanted vehicle within an ALPR system. First, ALPR systems allow for the manual entry of both a hotplate and a hotlist. Second, the ALPR system allows agencies to import National Crime Information Center (NCIC) records as an automated hotplate source. This is the most common method for populating hotlists.

Tactical vs. Investigative Uses

Law enforcement typically uses ALPR technology for both tactical and investigative purposes. Accordingly, agencies should consider both uses when developing their ALPR program's objectives. A tactical ALPR deployment includes placing cameras in strategically identified locations to generate information that warrants a rapid police response, such as stopping a wanted vehicle. These deployments usually seek to identify, locate, and recover a vehicle or its occupants to help address crime occurring in real time. An investigative use refers to utilizing ALPR cameras to collect license plate records that may have law enforcement interest but do not necessarily warrant an immediate police response. These detections are stored in the system and may later be queried. This information is generally used to create an investigative lead after a crime has occurred.

Business/Private Use

Since ALPR systems provide valuable data, private businesses and other organizations have also invested in ALPR technology. These uses may be for security, management, or operational needs. The following are examples of private sector use cases:

- Parking garages
- Hotels and casinos
- Homeowners associations
- Airports
- Convention centers
- Government traffic and transportation sites

2624

Program Design and Development

ALPR has proven to be a successful law enforcement tool. Its unique ability to provide actionable leads and help close cases cannot be overstated. However, real and perceived concerns exist regarding this technology's use. Therefore, law enforcement must take careful steps to develop an ALPR program that is both effective and appropriate. Taking a thoughtful approach when designing and developing these programs is the best strategy to accomplish these goals. Some of these considerations include developing proper policies, creating comprehensive training material, and designing and implementing responsible deployment strategies.

Policy Development

Establishing clearly defined policies on how ALPR may be used is the most effective method to minimize risk to the agency and protect both department employees and the individual rights of the public. ALPR policy should direct the purpose, general use, and processes involving ALPR investigations. These policies will provide a framework by which an agency can simultaneously reap the benefits of the technology, all while respecting the privacy and civil rights of the public. Similarly, consistent policies will assist in protecting the integrity of criminal investigations, criminal intelligence collection, and justice system processes. The following components should be considered while developing ALPR policies and procedures:

- Community-directed statement on why the agency is establishing or maintaining an ALPR capability
- The purpose of the policy
- General use guidelines of the technology
- Clearly defined program oversight roles and responsibilities
- The ALPR vendor and deployment types
- Access, training, and usage requirements
- Investigative procedure requirements
- Clear guidance to department employees on being transparent on the use and reporting of the technology in court documents
- Auditing responsibilities and schedule
- Data retention and purging
- Statement affirming protections for constitutionally protected activities
- Rules governing the use of hotplates

State/Local Law Considerations

Many state legislatures have taken steps to regulate the use of ALPR technology in their states. These laws and regulations can directly impact the functioning of an ALPR program in those states, and they must be accounted for in agency policy. Examples of the types of rules and regulations implemented in several states can be found in Appendix C – State-Level Laws and Regulations.

Training Considerations

Ensuring a thorough training program is in place is critical. Users must receive training on the ALPR system before receiving access. This practice ensures ALPR systems are only used for official law enforcement purposes consistent with applicable legal limitations and department policy. The training program should address several topics to ensure that users of an ALPR system are proficient in the necessary skills, including:

- A review of the departmental policy and safeguards related to ALPR use
- Basic understanding of how the technology operates
- The ALPR data sources, vendor, type of systems, etc.
- Any significant capabilities and or limitations related to the technology
- Any potential hazards related to the technology

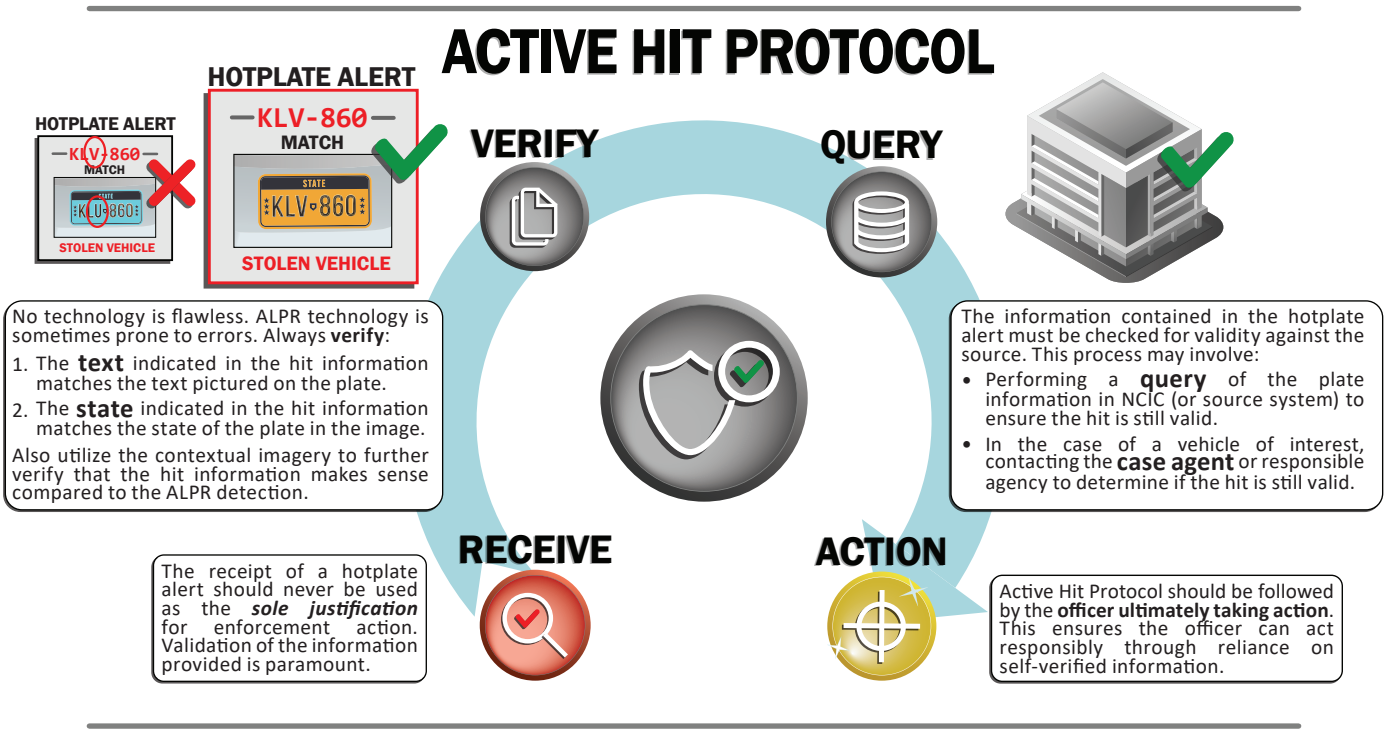
- Who is authorized to access the system and any required training
- The role of the officer or investigator in leveraging and responding to ALPR hotplate detections
- Importance of being transparent with arresting documentation
- Any applicable laws and policies that govern the use of ALPR in the specific jurisdiction
- Use of the ALPR system as an investigative tool
- The data retention period
- Auditing responsibilities

An ALPR training program should include a tactical-level discussion of how to use the technology appropriately. For mobile units, this should consist of an initial check to ensure that the ALPR system is operating correctly at the beginning of each shift. This includes logging into the system, running any necessary diagnostics to determine that it is working correctly, and doing a quick physical inspection of the system (cameras, cables, connections). In addition, a program manager should conduct periodic checks of fixed ALPR sites to verify that the hardware is operational and communicating with the software as intended.

Field Officer Responsibilities

A critical piece of the officer training on ALPR should include an element that instructs how ALPR notifications are processed and the appropriate response protocols for those notifications. Some departments may have fixed ALPR hits reviewed and confirmed by the public safety answering point or real-time crime center before dispatching them to an officer to investigate. Other systems may provide an in-car alert on the car computer system.

Officers should be required to review hotplate detection, confirm the detections, and appropriately respond to actively wanted vehicles. This process can be referred to as “Active Hit Protocol.”



Investigator Responsibilities

The ALPR system is a valuable investigative tool. It can be used to develop leads in cases involving vehicles where the license plate is unknown or to establish that a car was not in the vicinity during the time frame a crime occurred. An ALPR training program must include how to access the system and the criteria required before conducting a query, such as the reason for the search and the associated case number. Additionally, investigative tool training should address how to query the system, instructions on operating the various analytical tools within the system, how to interpret the data, how to preserve a record, and any required transparency, audit, or reporting requirements.

Types of Training

Training should be broken down into multiple categories:

- **New User Training:** This training will be detailed and define proper usage. In addition, this training should include policy, procedures, state and local laws, and an in-depth walk-through of the ALPR products and software.
- **Refresher Training:** This is considered a refresher of policy and procedures. It may also include changes to case law and examples of ALPR use. This training should ideally occur immediately after any changes to policy take place.

Authorized instructors should provide training on ALPR technology based on an established, accredited curriculum. An example of an accredited curriculum is one that has been approved by the state's Peace Officer's Standards and Training (POST) or equivalent body.

Deployment Strategies

Determining the ALPR deployment type and kind is one of the most critical decisions an agency will make concerning its ALPR program. Law enforcement is responsible for deploying advanced technology in a manner that is effective in its use and appropriate in its scope. Law enforcement also has a fiduciary duty to use public funds responsibly. For these reasons, ample consideration should be made when determining the type and kind of ALPR deployment.

ALPR Deployment Theories

As previously addressed, various types of ALPR technology exist, including fixed, mobile, portable, and smartphone applications, with each serving a unique purpose. Therefore, the kind of ALPR selected should be determined by the environment, infrastructure, and objectives for the ALPR deployment. Several ALPR deployment strategies are often considered when determining the value and placement of ALPR cameras. The most common of these strategies include the following:

- **High Traffic Areas:** The primary objective is to collect the maximum number of detections that can later be leveraged for investigative leads.
- **High Crime Areas:** This strategy focuses on producing information anticipated to be of investigative value instead of creating as many detections as possible.
- **Places of Interest:** This strategy is more of a hybrid between the first two. An example of this strategy would be deploying ALPR cameras around a shopping mall targeted by organized retail theft gangs or where assaults have occurred. Agencies may also place ALPR cameras in proximity to their community's major ingress/egress points and critical infrastructure or routes associated with gun, drug, or human trafficking.

Deployment Considerations

Infrastructure and permitting are two common factors that can limit an agency's deployment strategy for ALPR systems. Agencies must carefully consider each physical deployment site. The infrastructure to mount the necessary hardware must exist for the technology to be successfully deployed. Furthermore, the owner and operator of the infrastructure or property must allow for the installation of ALPR hardware. Agencies must also ensure that the proposed site is appropriate for the type of power the ALPR utilizes. Some systems run on AC power. While this provides constant and consistent power, installing it can be more expensive. Others rely on solar energy, which may only provide enough power if the camera site receives sufficient sunlight to account for the traffic volume. Finally, this infrastructure must have access to a data transmission service, such as cellular, fiber optic, or Wi-Fi.

Once a deployment plan has been established, site locations have been determined, and in-person inspections of the sites have been completed, the agency will need to navigate any legal and permitting processes. Since permitting can vary significantly across jurisdictions, it is recommended that agencies consult with their local public works or other appropriate governmental entities to ensure all necessary procedures are being met. Engaging these entities earlier in the process will help secure their buy-in, which will be critical for a successful deployment.

Equitability Concerns

Deployment strategies must account for concerns over bias, surveillance or other threats to privacy, and potential chilling effects on First Amendment, defendant, or related rights. The following recommendations will help ensure ALPR technology is deployed in a manner that supports just and equitable policing:

- Deployment plans should be informed by analyzing crime data, patterns, and trends. The site selection process should be based on this information and account for any relevant privacy, equitability, or other concerns.
- Agencies should consult the community, other stakeholders, and appropriate oversight committees. This includes providing specific information on why and how the deployment sites were selected.
- Deployment strategies should regularly be reviewed and evaluated to ensure the ALPR program and technology continue s to operate within the established guidelines and policies.

Partner Technologies

While developing the deployment plan, it is important to consider other law enforcement technologies that may complement the ALPR system. Law enforcement agencies may deploy complementary technologies within the same area, which have different capabilities. Agencies can leverage these capabilities to increase their ability to suppress crime, create actionable leads, solve cases, and potentially deter future crimes. Potential partner technologies can be subdivided into two categories: tactical and investigative.

Tactical technologies include tools such as gunshot detection technology, public safety cameras, and drone detection technology. An example of investigative technology is a records management system (RMS). Integrating ALPR and RMS can join plate reads to hotlists, allow investigators to search plate reads within a familiar interface, and provide a direct link between case management and the ALPR database. Another example of investigative technology is crime analysis software. Bringing ALPR data into an agency's chosen analysis software can aid in ongoing investigations. For example, agencies can import ALPR data to help create accurate timelines for vehicle travel that can provide investigators with unseen leads and valuable knowledge.

2628

Procurement

Responsible procurement of ALPR technology is a critical component of an effective program. The importance of obtaining stakeholder feedback early in the procurement process cannot be understated. Program managers should make every effort to embrace a spirit of transparency, accept critical feedback, and attempt to address any concerns raised by stakeholders directly.

The procurement phase is also the appropriate time to begin building departmental policies, procedures, and protocols, as this will be crucial in gaining stakeholder buy-in. It is imperative that the stakeholders understand how these policies will protect the public's privacy and civil liberties. Agencies should also seek to mitigate any concerns that stakeholders raise about the proposed ALPR program through thoughtful policy design.

Vendor and Product Assessment

Before choosing a vendor for their ALPR program, law enforcement agencies should conduct an appropriate degree of market research. This should include a trial of the product and conversations with existing customers to evaluate its performance in a real-world setting. A trial period provides the opportunity to test the technology, the associated policies and procedures, and highlight initial successes. This can provide tangible examples that can be shared with stakeholders to show how ALPR serves to enhance public safety.

Should an agency engage in a pilot program, it is recommended that the community be notified. Agencies should also determine how any information collected may be used in investigations or other law enforcement operations until a final protocol and all other areas of the program are formalized.

When determining the best hardware for their ALPR program, law enforcement agencies should consider the following:

- Hardware requirements for specific sites
- The lenses, processor, and other technical specifications of the hardware
- Average detections per hour
- General cost
- The number of lanes of traffic a single camera can capture
- The maximum speed at which the camera can read a license plate

When determining the best software for their ALPR program, law enforcement agencies should consider the following:

- The accuracy of the OCR software and whether it's enhanced by artificial intelligence, machine learning, or another capability
- The technology's alerting system, including desktop, laptop, mobile, app-based, and in-car alerts
- The software's ability to connect and share data with other law enforcement analytical platforms

Technical Challenges

There are some challenges with ALPR software that agencies must acknowledge. For example, OCR technology analyzes all letter or number sequences in the imagery; it cannot specifically isolate only license plate images. Therefore, a detection can be created on something that is not a license plate. This includes billboards, signage, marketing material on vehicles, etc. Additionally, the full license plate letter and number sequence must be visible to create an accurate license plate detection. Occlusion, missing plates, and temporary paper plates may result in no detection, a partial detection, or a misread.

Misreads may occur for several reasons, but most are due to the incorrect translation of a letter or number. For example, the system may read an "8" as a "B" or a "K" as an "X." These technical challenges should be readily acknowledged by both the agency and a prospective ALPR vendor. Agencies must ensure their policies account for these challenges and contain sufficient safeguards to limit instances where officers act based on a misread or other error.

2629

Procurement Ethics

While local procurement ordinances vary across jurisdictions, agencies must follow those ordinances along with broader guiding principles when procuring an ALPR platform. The National Institute of Governmental Purchasing's (NIGP) Values and Guiding Principles of Public Procurement are one such set of broad principles that agencies can use to inform any ALPR procurement process. The NIGP principles are as follows:

- **Accountability:** Taking ownership and being responsible to all stakeholders for our actions. This value is essential to preserve public trust and protect the public interest.
- **Ethics:** Doing the right thing. This value is essential to deserve the public's trust.
- **Impartiality:** Unbiased decision-making and actions. This value is essential to ensure fairness for the public good.
- **Professionalism:** Upholding high standards of job performance and ethical behavior. This value is essential to balance diverse public interests.
- **Service:** Obligation to assist stakeholders. This value is essential to support the public good.
- **Transparency:** Easily accessible and understandable policies and processes. This value is essential to demonstrate the responsible use of public funds.[3]

3 Additional information on NIGP's Guiding Principles can be found here: https://www.nigp.org/our-profession/values-and-guiding-principles-of-public-procurement

2630

Program Management and Oversight

An ALPR program's design and operational management are part of the framework of a successful program. Effective management and oversight of the program help ensure operational transparency and accountability and that ALPR technology is being used responsibly.

To ensure the program operates responsibly, agencies should assign a manager operational control of the ALPR program. This individual should be well versed in the technology, have a sound understanding of all significant components of the ALPR program, and be empowered to ensure the program follows protocols, policy, applicable law, and community and agency expectations.

A program manager's responsibilities include the following:

- Developing policies
- Overseeing training
- Ensuring appropriate use of the technology
- Managing data collection and reporting

A program manager is also responsible for staying current on technology changes and emerging ALPR trends. Similarly, they must ensure that their agency's ALPR policies and training are current and address technological changes or advancements. Finally, having a program manager establishes a clear point of contact between the law enforcement agency and the ALPR vendor. This can enhance the communication between the agency and vendor, which creates an opportunity to share and address any technological or other challenges.

Access and Appropriate Use

Law enforcement agencies are responsible for using ALPR data to uphold public safety, solve crimes, and prevent future crimes. Agencies have an opportunity to build public trust and support for the use of ALPR through transparency and responsible use. As such, agencies should carefully consider the circumstances under which using ALPR is appropriate and what personnel within the agency can access this tool.

Law enforcement agencies must scope their ALPR programs in a manner that ensures the agency is still able to conduct proper oversight and operate the program transparently. One method for achieving this is by limiting who can access the ALPR technology. For example, many law enforcement agencies restrict access to specialized personnel to ensure that the use of ALPR technology is adequately audited and controlled. Access should only be authorized once a user has completed the requisite training and demonstrates a baseline understanding and operational knowledge of the technology. Information on new user training, access, and use should be part of standard data collection and reporting related to the ALPR program.

Agencies that deploy ALPR must have written policies that outline the appropriate use of the technology. Several core principles should be incorporated into these policies to ensure the responsible use of the technology. First and foremost, ALPR technology should only be used as part of a criminal investigation or to address an articulable public safety concern. Secondly, the investigator must also have a legitimate "need to know" before querying any ALPR data. These guardrails will help prevent "curiosity checks" or other bad faith uses and ensure that privacy, civil rights, and civil liberties are respected.

Agency users must also demonstrate adherence to established policies when searching archived ALPR data. For example, if the ALPR software allows it, agency policy should require users to document the investigative purpose and case number associated with each query. Vague or ambiguous reasons for a search, such as "criminal subject" or "research," should be avoided. An agency's ALPR policies should also outline the potential consequences and corrective methods for improper use of the technology. Examples may include mandatory retraining, loss of access privileges, or other appropriate corrective punishments.

Data Retention

Data retention policies are ultimately determined by the agency using ALPR technology. These policies are informed by various considerations, including the agency's objectives, stakeholders' expectations, and local laws or regulations. Therefore, it is essential that the ALPR technology, vendor, and any other relevant service providers support the agency's policies on retention.

While a general best practice is not to retain data any longer than is necessary, what constitutes "no longer than necessary" is not a simple determination since different use cases may benefit from different retention periods. For example, cold cases may benefit from years-old data, while other uses rely on more recent data.

Outside of specified legal requirements, the retention schedule for ALPR data is primarily determined by agency policy.[4] As such, law enforcement must work with the community and other stakeholders to determine appropriate retention periods for each type of ALPR data. Ideally, ALPR systems should allow agencies to define retention schedules and automatically purge any record not designated for retention by a registered user. In addition, regular system audits ensure retention standards are followed and instill confidence that system data is utilized appropriately.

Data Sharing

For good reason, law enforcement agencies worldwide are embracing ALPR technology. A 2013 Bureau of Justice Statistics study showed that 77% of agencies serving populations of 100,000 or more have access to ALPR technology.[5] Moreover, given ALPR technology's value to a single jurisdiction, law enforcement has begun to explore sharing ALPR data across jurisdictional boundaries. Sharing ALPR data amongst law enforcement agencies fosters a more collaborative approach to addressing public safety concerns across jurisdictional boundaries.

Benefits of Data Sharing

When law enforcement agencies share ALPR data across jurisdictions, the technology can provide more comprehensive data. A shared system creates more unified and robust coverage throughout a region. Several ALPR vendors currently provide their law enforcement customer base with the ability to share data with other law enforcement customers. The potential to cross-reference information between separate ALPR systems allows law enforcement to enhance their investigative capabilities and can reveal elements of illegal activity that may otherwise be unknown to the investigating agency. Several elements of ALPR data and systems can be shared, including the ALPR detections and user-created hotlists. Some ALPR vendors also allow agencies to establish data-sharing relationships between their products and other technology systems.

As a standard practice, law enforcement agencies should consider sharing ALPR data with one another to the extent that state or local laws and regulations permit. Agency policy should define what, if any, type of data sharing is in place, who is authorized to establish data-sharing relationships, and any procedures that govern the sharing of ALPR data. These procedures and data-handling agreements should be implemented in policy for both the sharing and receiving agencies.

The success of ALPR technology among law enforcement has led non-government entities to acquire the same technology. This includes retailers, property managers, towing and repossession companies, parking lot operators, homeowner associations (HOAs), and even individual households. Since the generated data is of the same format and often targets issues of mutual interest, ALPR vendors have created Public-Private Partnership (PPP) friendly user interfaces. These programs typically allow the unidirectional sharing of ALPR data from the non-government side to the law enforcement side only. These partnerships strengthen community relationships and ensure public investments are used responsibly.

4 David J. Roberts and Meghann Casanova, Automated License Plate Recognition (ALPR) Systems: Policy and Operational Guidance for Law Enforcement, National Institute of Justice, U.S. Department of Justice, 2012. https://www.ojp.gov/pdffiles1/nij/grants/239605.pdf

5 B.A. Reaves, Local police departments, 2013: Equipment and Technology. Bureau of Justice Statistics, U.S. Department of Justice, July 2015. https://bjs.ojp.gov/library/publications/local-police-departments-2013-equipment-and-technology

2632

Data Sharing Considerations

While data sharing benefits agencies, safeguards are needed to protect the agency that generates and owns the data. Data sharing guidelines can be specific to the type of shared data. For instance, if agency "A" shares ALPR detection data with agency "B," there may be no requirement for a formal agreement. In contrast, if agency "A" shares hotplates or agency-generated hotlists with agency "B," this scenario may require a formal agreement. This is because hotplates or hotlists are typically generated from a criminal investigation or law enforcement process or function that may require an officer to take action if there is a confirmed detection. Furthermore, the agency that receives the information should bear the responsibility and liability for their officers' actions in response to an alert.

Law enforcement agencies seeking to share or receive ALPR data must be aware of applicable federal, state, and local laws. As such, agencies should consult with their legal representatives to identify pending, proposed, or existing laws that may be relevant. For example, legislation is proposed annually at all levels of government which, if enacted, could limit law enforcement data sharing. Finally, agencies must consider any concerns from the community or other stakeholders before establishing multi-jurisdictional data-sharing relationships.

Auditing, Data Collection, and Reporting

Auditing and reporting an agency's use of ALPR technology is a critical component of a transparent and accountable ALPR program. The failure to operate a program in this manner will only exacerbate concerns related to misuse or contribute to the perception that ALPR technology is synonymous with increased surveillance. This will undoubtedly negatively impact police-community relations. Agencies should develop robust mechanisms to evaluate the efficacy of the technology and ensure it is being used appropriately.

Auditing Requirements

Regular audits on an ALPR system are one method for validating compliance with agency policies and applicable laws and regulations. As with other reporting requirements, the specific auditing measures, and the frequency of said audits, should be clearly defined in the ALPR program's governance documents. In general, audits should verify what ALPR information was accessed and by whom, in order to identify any improper or unauthorized uses of this data. Audits should also ensure that data within the system is being handled per agency policy, including information sharing agreements. They should also confirm that data is being purged as required under any applicable data retention schedules.

Data Collection and Reporting Considerations

Studies have shown that ALPR technology is most effective when used systematically and when deployment sites are strategically selected.[6] In addition, comprehensive data collection and reporting will assist agencies with maximizing the benefits of ALPR technology. Finally, robust data collection and reporting will help increase transparency.

At a minimum, agencies using ALPR should collect and report the following information:

- Number of detections
- Number of hotplate hits
- Number of queries conducted by users
- Number of arrests directly attributed to ALPR hotplate detections
- Number of user-generated hotplates
- Breakdown of hotplate hit types
- Year-over-year analysis and trends

By analyzing this data, agency leaders and stakeholders can determine whether their ALPR system is meeting deployment goals and has significantly impacted crime or other areas of police operations. ALPR data collection and reporting also provide valuable insight into ALPR system adoption throughout the organization.

6 C. S. Koper and C. Lum, "The impacts of large-scale license plate reader deployment on criminal investigations," Police Quarterly, 22(3), 305–329, 2019. https://doi.org/10.1177/1098611119828039

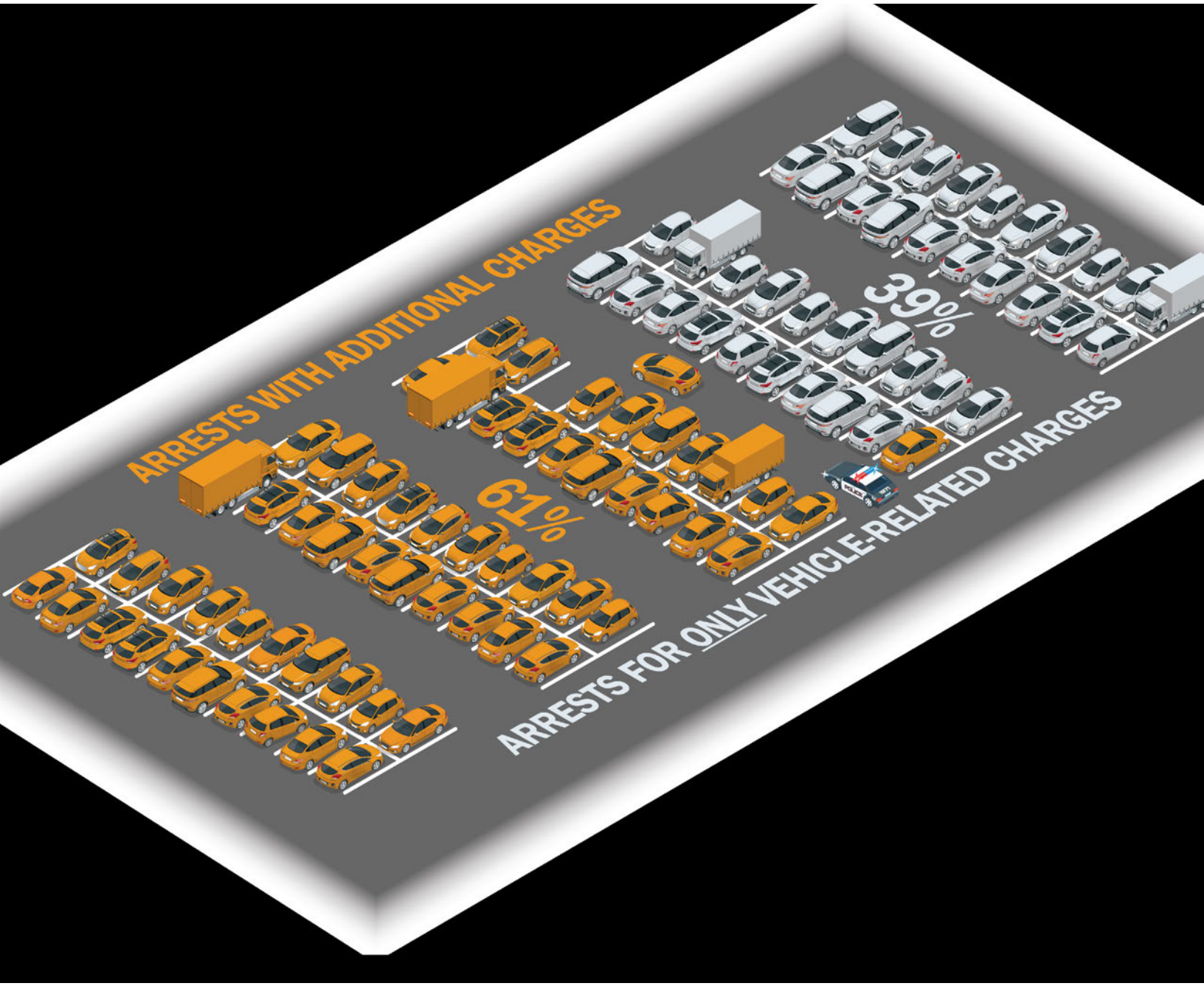
2633

The Importance of Analysis and Reporting

Quantitative data is an excellent tool to measure the impact of law enforcement technology. The ability to answer the questions “how many” and “how often” is necessary to evaluate real-world outcomes. Additionally, the quantitative analysis of ALPR data can provide an agency and stakeholders with the information needed to determine the impact of the technology on community safety.

To explore the potential of quantitative reporting, an MCCA member agency recently analyzed the impact of a localized ALPR deployment. The data presented below represents a period of four months after the installation of ALPR cameras within the evaluated area. The types of charges related to any arrests resulting from an ALPR event were analyzed. The data suggests that ALPR technology generates leads and solves more types of crimes than those related to ALPR’s most frequent use: the recovery of stolen vehicles.

It is important to capture and analyze the impact of any ALPR program to dispel misconceptions and demonstrate the impact of the technology.



2634

Data Stewardship

Throughout the design of an ALPR program, the hardware, software, and policies implemented will shape how ALPR data is collected and stored. Therefore, a comprehensive strategy should be developed to ensure all data collection aspects are secured and managed effectively.

Data Roles and Responsibilities

ALPR records are typically stored in databases that can be indexed, searched by individual or composite conditions, and analytically processed by applications that power ALPR use cases. This is an important and powerful compilation of data that must be managed judiciously. The two primary roles relative to this data are data owners and service providers.

The data owner is the organization that controls the data and decision-making authority. The data owner, typically the data's generator and user, determines how the data may be used, who it can be shared with, and its retention limits. For example, law enforcement is always the data owner for the ALPR data it generates. While this data may be shared with other law enforcement entities, the owner and provider of any particular data always retains control over all aspects of it. Therefore, other organizations that have received access to that data must act in accordance with the data owner's direction, such as adhering to retention limits established by the owner on the data.

A service provider is an entity that may take possession of data to store or process it on behalf of the data owner. The service provider operates at the behest of the data owner and enacts the owner's wishes and directions. This can include management of data sharing with other designated users, enforcing retention limits, etc. The service provider has no entitlement to the data and may not sell, derive secondary insights, or otherwise share it. Furthermore, they may only access the data to perform a function at the direction of the data owner. Law enforcement agencies often hire an outside company to be their service provider for ALPR data.

Storing and Processing ALPR Data

There are several general models for storing and processing ALPR data:

- The data is stored on-premises and processed by applications under the direct physical control of the organization that generates and uses the data.
- The data is stored off-premises by a cloud service provider and processed by applications in the cloud or on-premises under the direct control of the organization that generates and uses the data.
- The data is stored in the cloud or at an off site data center and is processed by a service provider.

In the first model, the data owner is effectively their own service provider, and there isn't necessarily a third party service-providing entity. The other two models imply some degree of a third party service provider. In those cases, the data may be held or accessed by another entity on behalf of the data owner. For ALPR systems, this could be either a cloud computing service or an ALPR technology vendor. However, in both cases, control of the data remains with the data owner.

Data Security

Law enforcement agencies should treat ALPR data like any other sensitive data it collects, uses, and manages. It should be protected as judiciously as law enforcement records, video, and other critical operational data. This includes ensuring responsible usage of the data by law enforcement personnel and vetting any service providers that may process the data. Law enforcement agencies must also apply rigorous cybersecurity practices to protect and secure the ALPR data it generates and uses. This includes, but is not limited to, proper authentication methods (multi-factor authentication is generally considered a best practice), data-sharing controls, and role-based access controls for users. Law enforcement agencies must ensure that their technology vendors provide adequate security practices to protect the ALPR data they possess and process on behalf of the agency.

Whether a service provider provides on-premise technology, stores data on behalf of a law enforcement agency, or hosts the processing applications, they have an important role in ensuring the secure and trustworthy operation of an ALPR program. The service provider is responsible for securing the data it processes to protect it from unauthorized access, theft, or misuse. They must provide the necessary capabilities, controls, and training to enable law enforcement agencies to enforce their own defined data governance policies, security standards, and procedures. This includes:

- **Enforcement of Retention Limits:** This may be applied absolutely or in a role-based fashion. For example, the absolute retention limit for ALPR data could be three years, but only cold case investigators may access data older than six months.
- **Positive Controls Over How Data is Shared:** Data must only be shared after law enforcement specifically enables it with individual partners at its discretion and under the auspices of its policies.
- **Enforcement of Personnel Controls:** These controls include system and user-level authorization, role-based access controls, and regular audits.

The FBI's Criminal Justice Information Services (CJIS) Security Policy provides a comprehensive reference and standard that agencies may use to design or measure data management for their program. For cases where service providers take possession of ALPR data from law enforcement agencies to store and process on their behalf, agencies should consider using the CJIS Security Policy to assess and set expectations of service providers.[7] An explanation of relevant sections of the CJIS Security Policy can be found in Appendix D – CJIS Security Policy.

As mentioned earlier, cloud services may be part of an agency's ALPR program. These services' security and integrity depend on the efficacy of the underlying cloud platform. Cloud service providers (or service providers that operate their own data center directly) should comply with ISO 9001:2015, an internationally recognized standard for Quality Management Systems. Compliance with this standard should be independently audited and verified for compliance under the Statement of Auditing Standards Number 70 [SOC 2 Report]. In addition, compliance with FedRAMP medium security controls provides an additional level of validation and may be required for information sharing with federal entities. Even though license plate detection records are not personally identifiable, they may be linked through other sources that may enable the end user to input data that could be viewed as personally identifiable or criminal justice information.

ALPR Reader Device Integrity

An ALPR reader that captures ALPR images and does local image processing contains instances of ALPR data. This data may be transient or stored on the device for extended periods. Since ALPR readers are often distributed in the environment and may be difficult to physically secure, it is increasingly important to consider the device's ability to locally secure ALPR data that is either at rest or in motion. FIPS (Federal Information Processing Standards) 140 standards are used to evaluate the hardware and software integrity of cryptographic modules. This applies to many devices, including ALPR readers, that need to encrypt data to secure it from compromise. FIPS 140-2 is broken into four, successively increasing levels of security.[8]

- FIPS 140-2 Level 1 is the lowest and imposes limited requirements.
- FIPS 140-2 Level 2 adds requirements for physical tamper-evidence and role-based authentication.
- FIPS 140-2 Level 3 adds requirements for physical tamper-resistance (making it difficult for attackers to gain access to the sensitive information contained in the module) and identity-based authentication, and for a physical or logical separation between the interfaces by which "critical security parameters" enter and leave the module, and its other interfaces.
- FIPS 140-2 Level 4 makes the physical security requirements more stringent and requires robustness against environmental attacks.

Depending upon the specific environment where it is deployed, the ALPR reading device should, at a minimum, support FIPS 140-2 Level 2. Aspects of FIPS 140-2 Level 3 are also becoming increasingly desirable and necessary, especially as ALPR technology advances.

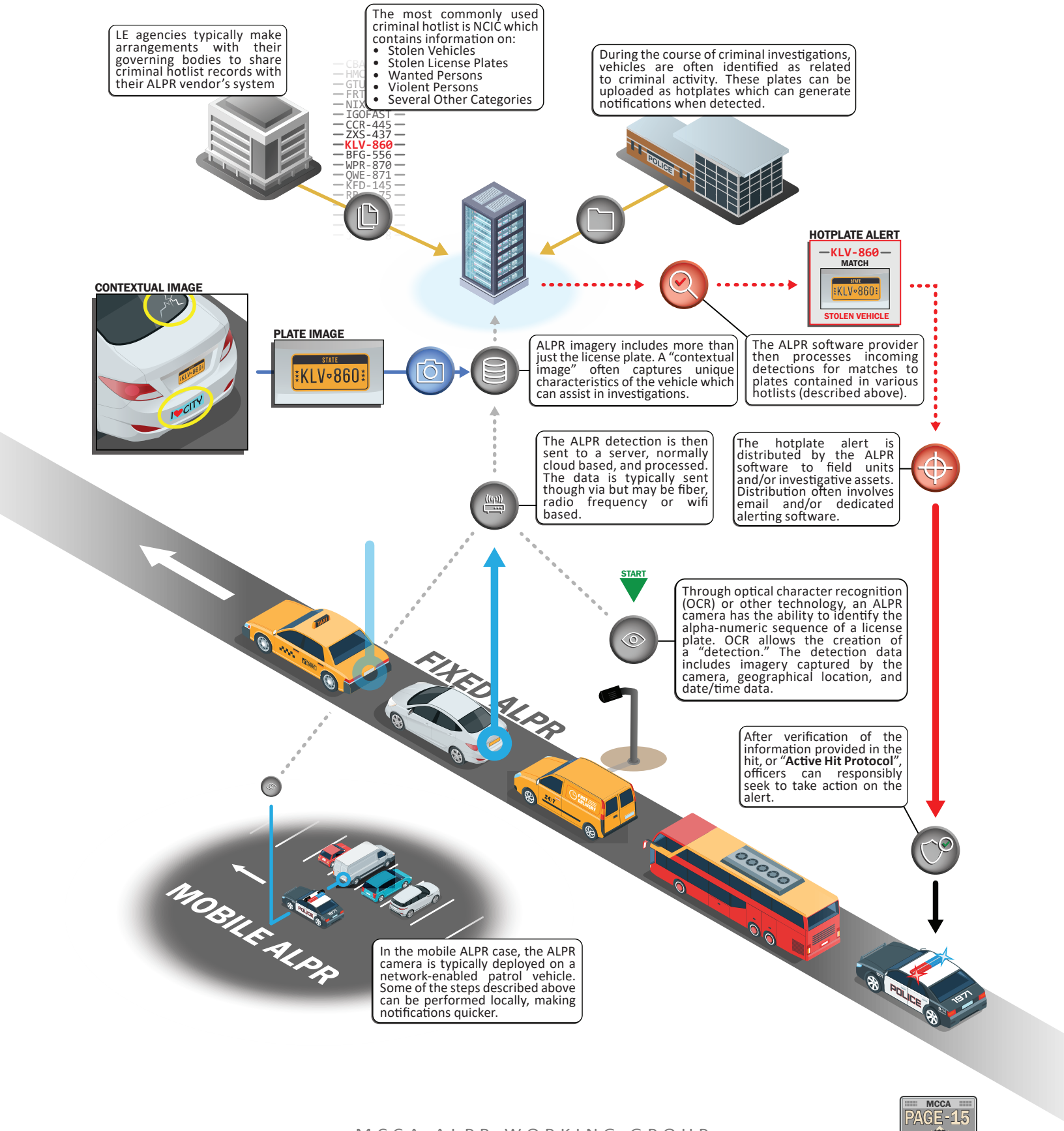
7 Criminal Justice Information Services (CJIS) Security Policy, CJISD-ITS-DOC-08140-5.9.1, US Department of Justice - Federal Bureau of Investigation, Version 5.9.1, October 22, 2022.

8 A. Lee, M. Smid, S. Snouffer, Security Requirements for Cryptographic Modules [includes Change Notices as of 12/3/2002], (NIST FIPS), National Institute of Standards and Technology, 2001. https://doi.org/10.6028/NIST.FIPS.140-2

2636

ALPR Operations Infographic

Several aspects of the operation of ALPR technology can be better understood when put in the context of the technological workflow.



2637

ALPR Synergy with Other Law Enforcement Technologies

As law enforcement gains access to more information, technology will help ensure the data is organized so law enforcement officers can solve complex policing problems. Any single data source, such as ALPR, only answers one of many questions. It only tells law enforcement where a vehicle was at a given time. ALPR alone does not answer critical questions such as whom the car belongs to or who has been associated with it before, whether any of those individuals have a history of involvement in similar incidents, and other critical questions.

By integrating data across common law enforcement data sources, those questions can be asked and answered immediately, drastically increasing the odds of solving cases. Here are a few examples:

> *Consider a situation where CCTV footage captures a partial plate on a vehicle shortly after the commission of a crime. In an ideal scenario, an ALPR database may be queried to determine the rest of the characters on the license plate. Then a separate RMS system could be queried to determine if that license plate has ever been mentioned in a case report.*
>
> *A platform has ALPR, RMS, citation, and crash data integrated into one place. An ALPR detection can be searched and then linked to see if that plate has been named in an RMS case, vehicle citation, or crash report, along with any involved individuals. Links between vehicles, people, and incidents can be seen without having to search each database individually.*
>
> *An ALPR alert occurs in a platform that has CAD & CCTV integrated. As a result, an immediate CAD call can be created to accompany the alert, and any relevant CCTV footage in the area can be attached and sent to the responding officer, better preparing them to engage with the vehicle that triggered the alert.*

In these examples, a singular piece of information would have failed to fully identify the suspect vehicle. It is the utilization of an ALPR database in conjunction with other technologies produces an actionable investigative lead. For ALPR detections to be used to their fullest potential, that data must be connected to other relevant data sets.

The ultimate goal of connected data should be to allow for insights that are impossible to see currently or take too much time to consider. Departments should own all their data, including ALPR detections, and be able to link, connect, or integrate data sets as department leadership deems appropriate. When developing an ALPR program, agencies should ensure their vendors are aligned with this perspective and are capable of facilitating integrations with other law enforcement technology.

Beyond ALPR: AI-Enhanced Vehicle Detection

With advances in image processing technology, specifically those afforded by artificial intelligence and machine learning, it is becoming increasingly possible to identify a vehicle solely from an image. Artificial intelligence is able to focus on characteristics of a vehicle such as make, model, color, or distinguishing attributes/markings. These advanced image processing technologies improve the accuracy of ALPR systems and allow law enforcement to corroborate ALPR information. For example, they could assist with confirming that the vehicle associated with a detection matches the description in the registration record. Image-based detection and identification will continue to advance and improve the efficacy of ALPR technology.

2638

Case Law Related to ALPR

License plates are required in every state to display proof of registration. Registration identifies a particular vehicle and confirms that it meets minimum state-mandated safety requirements to be operated on public roadways. In addition, operators of vehicles must be licensed to drive legally on public roads.

It is possible in many states to own a vehicle and, if it is never parked or operated on a public roadway, not be required to display license plates. Furthermore, one can own a car but have no authority to operate it, just as one can be licensed to drive a car but never actually own one. Collecting information related to people and vehicles are separate and distinct concepts, although not entirely mutually exclusive. The alpha-numeric characters of a license plate alone do not indicate who owns the vehicle or is licensed to operate it.

For more than 50 years, the United States Supreme Court, and many lower courts, have repeatedly acknowledged that vehicles are inherently subject to greater regulation when operated on public roadways. In the age of enhanced technology, ALPR invokes specific legal considerations:

- Reasonable privacy expectations of those in vehicles on public roadways
- Persistent tracking and the nature of ALPR technology
- The nexus between license plates and personally identifiable information
- Collecting and sharing ALPR data
- The degree of intrusion authorized by an ALPR hotplate detection

An examination of existing case law related to these concepts follows. There is often no bright-line precedent when considering emergent technology. In such instances, reasonable legal conclusions can be inferred from cases related to other technology and privacy issues already adjudicated by the courts.

Privacy Expectations on Public Roadways

In 1967, the U.S. Supreme Court clarified in *Katz v. U.S. (1967)* that "the Fourth Amendment protects people, not places." [9] The Fourth Amendment of the United States Constitution ensures:

> *[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.*

In *Cady v. Dombrowski (1973),* the U.S. Supreme Court noted that vehicles, while "effects," are constitutionally different from a person's home. The case also referenced the regularity with which police engage in activity unrelated to the enforcement of laws, such as maintaining the efficiency of the flow of traffic and ensuring the safety of those using the roadways. The Court acknowledged that this regular contact with automobiles contributes to police being more often in "plain view" of evidence, instrumentalities of a crime, or contraband.[10]

Delaware v. Prouse (1979) offers historic guidance concerning the constitutionality of stopping or seizing vehicles. The U.S. Supreme Court cites, "the permissibility of a particular law enforcement practice is judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests."[11] One can reasonably infer that photographing a plainly visible license plate, on a public roadway, or from a location plainly visible from a lawfully authorized location, with no intrusion upon the vehicle occupants or otherwise interfering with their movement or affecting any person's possessory interest in the vehicle or license plate, is not a seizure constitutionally.

Lower courts have routinely ruled that law enforcement officers may, without specific suspicion, check the status of a license plate against a law enforcement database.[12][13] Therefore, searching aggregated photographs, which contain no specific information about a particular vehicle owner or operator, even when correlated with additional information such as the time, date, and location of the photograph, does not constitute a search.

9 Katz v. United States, 389 United States Supreme Court. 347, (1967). https://supreme.justia.com/cases/federal/us/389/347

10 Cady v. Dombrowski, 413 United States Supreme Court. 433 (1973). https://supreme.justia.com/cases/federal/us/413/433

11 Delaware v. Prouse, 440 United States Supreme Court. 648 (1979). https://supreme.justia.com/cases/federal/us/413/433

12 Jones v. Town of Woodworth, Court of Appeal of Louisiana. 15-568. (2015). https://caselaw.findlaw.com/la-court-of-appeal/1717448.html

13 State v. Davis, 237 Or. App. 351, 239 P.3d 1002, Oregon Court of Appeals. (2010). https://caselaw.findlaw.com/la-court-of-appeal/1717448.html

Is ALPR Persistent Tracking?

The notion that vehicle travel on public roadways is an unavoidable element of modern living merits consideration, given how ALPR is deployed. Recent U.S. Supreme Court rulings related to law enforcement's use of other technologies have considered the inescapable and automatic nature of data collection. An analysis of these rulings is offered to differentiate the substantially greater capabilities of such technologies compared to those of ALPR.

Two recent U.S. Supreme Court rulings merit particular consideration for the use of technology to investigate the historical movement of persons. In *U.S. v. Jones (2012)*, the U.S Supreme Court held that police need a search warrant to install a covert GPS tracking device on a vehicle to monitor its location for an extended period of time. In *Carpenter v. U.S. (2018),* The Court ruled that police must secure a warrant before obtaining cell-site location information from service providers regarding an individual's location history.

The theme of both cases concerns the capacity that modern technology affords the government to explore comprehensive, specifically personal location information, which was not possible until the advent of recent ubiquitous technology. GPS and cell-site location information enable persistent automated tracking of a targeted individual's activity with such detail and scope that the techniques constitute a search. In the case of *Carpenter v. U.S. (2018),* the Government obtained 12,898 location points cataloging Carpenter's movements. This extensive amount of information amounted to an average of 101 data points per day during the period they obtained historical records.[14]

An ALPR system cannot independently predict life patterns accurately or be used to conduct real-time surveillance of any person or vehicle. Even if police acted with willful disregard for the protections of the Fourth Amendment, it is impossible to accomplish such a degree of ongoing surveillance using ALPR technology. A fixed ALPR camera may be able to collect information about every car that passes its location. Still, the data is limited to an otherwise anonymous characteristic of the vehicle, not automatically attributable to any individual without accessing other restricted databases, and for only a single moment in time at a single location.

Images of plates stored in the ALPR database are retained and made available for specified queries. Tangential information may include the nature of a vehicle's location, direction of travel, and any criminal justice information associated with the detection. As to the question of whether a collection of images from multiple cameras, aggregated in a searchable database implicates Fourth Amendment considerations, the US Supreme Court has not taken up precisely to what extent ALPR coverage, or how robust an ALPR database is, may trigger specific Fourth Amendment implications.

In *Commonwealth v. McCarthy (2020)*, the Massachusetts Supreme Judicial Court concluded that "While the defendant has a constitutionally protected expectation of privacy in the whole of his public movements, an interest which potentially could be implicated by the widespread use of ALPRs, that interest was not invaded by the limited extent and use of ALPR data in this case." The case involved law enforcement's use of four ALPR devices on two bridges to investigate a defendant's movements during a period of two months. In that case, the court ruled that the limited use of ALPR data did not violate the defendant's reasonable expectation of privacy.[15]

License Plates & Personally Identifiable Information (PII)

Individuals (people) are licensed, but a vehicle is registered. A vehicle is registered with an organization (typically a state), which then authorizes the vehicle to be driven on public roads and highways by a licensed driver. For example, passenger and commercial vehicles must be registered as a condition of use on a public thoroughfare. Upon registration, the state department of motor vehicles then issues a license plate which must be attached to the vehicle and openly displayed for vehicle identification purposes. The purpose of a license plate is to identify a vehicle uniquely, and it does not include personally identifiable information of any individual. By itself, a license plate number is an anonymous code unless combined with other registration information containing owner/operator information (i.e., a department of motor vehicles database or an employee or homeowner registration). Thus, an ALPR record is generated from publicly available data and corresponds with detecting a vehicle, not an individual, at a specific location and time.

The federal *Driver's Privacy Protection Act (DPPA)* was enacted in 1994 to "protect the personal privacy and safety

14 Carpenter v. United States, United States Supreme Court. 585 (2018). https://supreme.justia.com/cases/federal/us/585/16-402

15 Commonwealth v. McCarthy, 484 Massachusetts Supreme Judicial Court (2020). https://cases.justia.com/massachusetts/supreme-court/2020-sjc-12750.pdf

2640

of licensed drivers consistent with the legitimate needs of business and government." DPPA made it "unlawful" to access, disseminate, or otherwise misuse information held by a state's motor vehicle office, including information related to both drivers and vehicles, without the owner's consent or for another legitimate, legally authorized purpose, such as criminal justice purposes. ALPR systems do not automatically link to data governed by DPPA. Law enforcement can only obtain such protected information from other secure, access-restricted criminal justice databases.

The case of *Harrison Neal v. Fairfax County Police (2020)* examined the use of an ALPR system to passively scan and retain license plates that were not on a hotlist to determine if such a practice violated the state's *Government Data Collection and Dissemination Practices Act.*

A key element of the case was whether an ALPR system constitutes an information system governed by the Code of Virginia. The court found that the ALPR system did not, noting that the ALPR database can be searched only by license plate number, not by any person's information. Furthermore, the system does not gather identifying information about the vehicle owner. To acquire such personal data, an officer must query a wholly separate criminal justice database via a different computer program.[16]

California Code 1798.29 specifically expands the meaning of "personal information" to include information or data collected through the use or operation of an ALPR system. While not adjudicated by any court, ALPR information is considered personal information in California due to unique state legislation.

Data Collection & Sharing

A license plate is a required government instrument specifically intended to identify the vehicle to which it is affixed publicly. In the case of *United States v. Ellison (2006)*, the Court noted:

> *This court has yet to address in a published opinion the question of whether an individual has a reasonable expectation of privacy regarding their license plate. In two unpublished decisions, however, this court has agreed with the other circuits that have decided this issue by holding that no such privacy interest exists. The reasoning of these opinions, as well as that of the Supreme Court in related cases, leads us to agree that a motorist has no reasonable expectation of privacy in the information contained on his license plate under the Fourth Amendment.[17]*

Publicly viewing or photographing a displayed license plate constitutes activity protected by the First Amendment of the United States. The cataloging and subsequent sharing of such data remain largely regulated by state or local legislation. In the case of *U.S. v. Yang (2020),* the Ninth Circuit ruled that the defendant did not have standing to challenge government queries of a vendor's ALPR database for records of his movement when he kept a rental car beyond the contract due date. The court noted that Yang failed to establish that he had a reasonable expectation of privacy in the historical location information of the vehicle that was the subject of the query. The Court declined to address any potential privacy interests related to the warrantless use of ALPR technology.[18]

16 Harrison Neal v. Fairfax County Police, Record No. 191127, Supreme Court of Virginia (2020). https://cases.justia.com/virginia/supreme-court/2020-191127.pdf

17 United States v. Ellison, 462 F.3d 557, 561, United States Supreme Court. (6th Cir. 2006). https://caselaw.findlaw.com/la-court-of-appeal/1717448.html

18 United States v. Yang, No. 18-10341, United States Court of Appeals for the 9th Circuit (2020) https://law.justia.com/cases/federal/appellate-courts/ca9/18-10341/18-10341-2020-05-04.html

2641

ALPR Hits & Degrees of Intrusion

Several cases have affirmed that an ALPR hotplate detection, also referred to as a "hit," constitutes sufficient reasonable suspicion to affect a traffic stop. For example, in the case of *Hernandez-Lopez v. State (2013)*, the Georgia Court of Appeals held that an ALPR system merely aided the officer by augmenting his sensory faculties and that based on the alert provided by the ALPR, the officer had reasonable, articulable suspicion to conduct a traffic stop. [19]

Similarly, in the case of *Traft v. Commonwealth (2018)*, the Supreme Court of Kentucky held that an officer obtaining information linked to his license plate did not violate the defendant's rights under the Fourth Amendment. This information indicated that Traft had an outstanding bench warrant and, therefore, reasonable suspicion existed to stop the vehicle. Furthermore, the court noted that the license plate "was displayed in a place where he had no reasonable expectation of privacy."[20]

In the case of *Green v. City and County of San Francisco (2014)*, an ALPR system returned a hit based on a misread. The officer was transporting a prisoner at the time and could not verify the hit's validity. The image on the ALPR was "dark and blurry." The officer subsequently provided a description of the vehicle via police radio, including the incorrect license plate indicated by the ALPR system, not the actual plate displayed on the car. Dispatch ran the plate as provided and noted that it belonged on a pick-up truck.[21]

A second officer observed Green's sedan bearing the plate as broadcast by the first officer. However, this officer also failed to confirm whether the radioed license plate number matched the plates on Green's car. Consequently, Green was stopped, challenged at gunpoint by multiple officers, placed on the ground, and handcuffed. Green filed suit against the defendants, alleging claims under 42 U.S.C. 1983 and California state law for wrongful detention, false arrest, and excessive force. The Ninth Circuit ruled that "an unconfirmed hit on the ALPR does not, alone, form the reasonable suspicion necessary to support an investigatory detention."

While legally permissible to affect a stop based on an ALPR hit, independent verification of the validity of an ALPR alert should be considered a best practice. Verifying that the actual vehicle license plate and the read on the ALPR screen are safeguards against a potential unjustified intrusion upon any person. Such guidance should neither cause officers to hesitate when officer safety is a concern nor preclude officers from acting on indicators amounting to reasonable suspicion based on other observations coupled with their training and experience. However, inappropriate outcomes resulting from the use of law enforcement technology can have substantial repercussions on perceptions of police legitimacy and the continued availability of such tools.

In conclusion, ALPR systems detect license plates in public locations collecting information that is generally not considered private. Critical elements of an ALPR system, such as the extent of camera coverage, reasons for selecting fixed deployment locations, length of time that data is retained, and the extent to which the information is shared, may factor in with respect to if an ALPR system implicates Fourth Amendment considerations. The consistently responsible use and thoughtful deployment of ALPR technology will ensure that all civil rights and liberties are respected.

19 Hernandez-Lopez v. State, 319 Ga. App. 662, 738 S.E.2d 116, Court of Appeals of Georgia (2013) https://cite.case.law/ga-app/319/662

20 Traft v. Commonwealth, 539 S.W.3d 647 Supreme Court of Kentucky (2018) https://cite.case.law/ga-app/319/662

21 Green v. City and County of San Francisco, No. 11-17892, United States Court of Appeals for the 9th Circuit (2014). https://law.justia.com/cases/federal/appellate-courts/ca9/18-10341/18-10341-2020-05-04.html

2642

Conclusion

As stated in the introduction, this product contains suggestions and recommendations, which, if adopted, will maximize ALPR technology's effectiveness while ensuring it is used ethically and responsibly. While this product provides a robust evaluation of the technology, it is impossible to cover every aspect of the technology. Therefore, the Working Group recommends that law enforcement use the tenets discussed in this document to help evaluate decisions regarding the use of ALPR technology. This must include the potential impact of ALPR technology on public trust and the community served. It is essential that, when implementing any technology program, law enforcement operate in a manner that is thoughtful, disciplined, and contextually mindful of its constituencies.

For those agencies wishing to implement an ALPR program but are still determining how to move forward, collaboration with other entities who have already developed robust, responsible programs is recommended. The sharing of best practices in crime-fighting technology among law enforcement has a history of beneficial impacts. Law enforcement must be good stewards of information and policies and be willing to share this with fellow law enforcement agencies wishing to begin using ALPR.

Law enforcement's use of ALPR is ubiquitous because the information these systems provide is advantageous. ALPR data has aided in countless successful criminal investigations and has proven to be one of the most valuable technologies available to law enforcement. Few technologies have aided law enforcement in keeping communities safe like ALPR. However, the capabilities of ALPR technology are continuously evolving, and the MCCA will continue to monitor it. The MCCA will remain engaged with all interested stakeholders and communicate the latest information with member agencies and the entire law enforcement profession so best practices can be adjusted as needed.

2643

Acknowledgments

Major Cities Chiefs Association would like to extend a special thanks to the ALPR Working Group and its members listed below. The contents of this document would not be possible without the collaboration between these law enforcement professionals and the technology vendor participants.

Kelly Bluth
DETECTIVE
Las Vegas Metropolitan Police Department

Blake Bullock
SENIOR DIRECTOR & GM FLEET PRODUCTS
Axon

Paige Burley
CLIENT FACING DEPLOYMENT
Peregrine

Gabriel Candelaria
LIEUTENANT
Dallas Police Department

Jeffrey Carroll
ASSISTANT CHIEF OF POLICE
Metropolitan Police Department Washington D.C.

Laura Cooper
EXECUTIVE DIRECTOR
Major Cities Chiefs Association

Travis Eicher
LMPD TECHNICAL SERVICES
Louisville Police Department

Dan Gillespie
TECHNOLOGY PROGRAM MANAGER
Louisville Police Department

Jeremy Harrison
MAJOR
Oklahoma City Police Department

Kyle Hoertsch
PRODUCT DEVELOPMENT MGR ENTERPRISE SOLUTIONS
Motorola Solutions

Milton Wyatt Martin
ASSISTANT CHIEF
Houston Police Department

Matt Melton
SENIOR BUSINESS DEVELOPMENT MANAGER
Amazon Web Services

Jason Olin
DIRECTOR OF GOVERNMENT AFFAIRS
Major Cities Chiefs Association

Samuel Paul
DEPUTY
Los Angeles Sheriff's Department

Christian Quinn
MANAGING PRINCIPAL
Fulcrum Innovation LLC

Jeremy Slavish
SENIOR BUSINESS DEVELOPMENT MANAGER
Amazon Web Services

Paul Steinberg
SENIOR VICE PRESIDENT OF TECHNOLOGY
Motorola Solutions

Josh Thomas
VP OF POLICY AND COMMUNICATIONS
Flock Safety

Matthew Thomas
COMMANDER
Indianapolis Metropolitan Police Department

Mark Torres
COMMANDER - REAL TIME CRIME CENTER
Albuquerque Police Department

Mike Wagers
SENIOR VICE PRESIDENT STRATEGIC INITIATIVES
Axon

Dalton Webb
DIRECTOR OF RTCC STRATEGY
Flock Safety

Paden Weber
INTELLIGENCE OFFICER
Las Vegas Metropolitan Police Department

William Zelms
CAPTAIN
Virginia Beach Police Department

GRAPHIC DESIGN BY PADEN WEBER

2644

Definitions

Automated License Plate Reader/Recognition (ALPR): ALPR systems comprise cameras that capture an image of a vehicle's license plate and use Optical Character Recognition (OCR) to automatically read license plate characters.

Contextual Photo/Image: An overview image of the area around a detection.

ALPR Record/Detection: Is generated when an instance of a vehicle license plate is detected, imaged, and processed to identify the plate.

Hit: A detection of a license plate that matches a plate previously registered on a hotlist or hotplate.

Hotlist: A file that contains the license plate numbers of stolen vehicles; AMBER, SILVER, or other law enforcement alerts; lists of license plate numbers known to be associated with specific individuals, such as wanted or missing individuals.

Hotplate: A license plate with a wanted status. It may also be entered into a system designed to provide a notification of future detections.

Misread: An incorrect translation of a license plate.

Fixed Camera: An ALPR camera that is affixed to a non-moving structure.

Mobile Camera: A vehicle-mounted camera.

Law Enforcement Data: ALPR data collected by law enforcement-owned ALPR cameras.

Data Retention: Refers to the amount of time that the collected data will be preserved.

Personally Identifiable Information (PII): Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.[1]

National Crime Information Center (NCIC): An electronic clearinghouse of crime data, such as mug shots and crime records, available to virtually every criminal justice agency nationwide.[2]

1 Guidance on the Protection of Personally Identifiable Information, U.S. Department of Labor. https://www.dol.gov/general/ppiihttps://www.dol.gov/general/ppii

2 National Crime Information Center (NCIC), Federal Bureau of Investigation. https://le.fbi.gov/informational-tools/ncic

2645

Appendix A – Success Stories

Homicide

After committing a homicide, the suspect fled the scene by vehicle. During the investigation, investigators learned that the suspect drove a specific vehicle with damage to the body. Using the ALPR system, detectives created a geographic boundary around the crime location. While reviewing the historical ALPR detections from that immediate area, a vehicle matching the suspect's vehicle description was identified. Detectives then discovered the actual license plate registration information, which returned to the primary suspect. Another query of that vehicle through the ALPR system revealed that the suspect vehicle had fled the jurisdiction immediately after the homicide occurred. This was later confirmed and corroborated by the suspect's cell phone location records.

Homicide

During a road rage incident resulting in a shooting and murder, the suspect was reportedly driving a black hearse. Responding officers obtained the victim's license plate number and checked it through the ALPR system. The officers located an ALPR record of the victim's vehicle passing an ALPR deployment site three minutes before the shooting. The officers checked for other vehicles driving past the ALPR cameras around the same time as the victim. The vehicle driving directly behind the victim was a black hearse. The ALPR data, along with a tip from the public, were pivotal in the arrest. The suspect gave a full confession. The arrest occurred within only a few hours of the crime.

Homicide

The victim knocked on the suspect's hotel room door. Annoyed by the knocking, the suspect opened the door and immediately shot and killed the victim. Surveillance footage of the suspect and his associate leaving captured the type of vehicle used by the suspect but did not capture the license plate. An ALPR camera system was stationed just down the street from the hotel. Officers reviewed the ALPR database for the time frame around the homicide. One minute before the 911 call, the ALPR camera captured a detection of a vehicle matching the one observed in the hotel surveillance. Armed with the vehicle registration information, the vehicle's lien holder was contacted, which provided new investigative leads. Within 11 hours of the shooting, officers located the suspect's vehicle hidden in a home's garage. The suspect and his associate were detained, provided a confession, and later charged with homicide.

Burglary

A police agency used ALPR to identify two suspect vehicles involved in a burglary. Multiple suspects in two vehicles committed a residential burglary, with the resident shooting and killing one of the suspects. Doorbell camera videos were recovered, and homicide detectives used them to establish a timeline. ALPR searches focused on the timeline, which resulted in ALPR scans for both suspect vehicles. A subject associated with one of the vehicles was later determined to be involved and arrested for burglary.

Sexual Assault and Attempted Murder

A victim met the suspect at a bar. They left and the suspect drove them to the desert, where he sexually assaulted, beat, strangled, and ran her over. The vehicle plate from the bar where the incident began was queried in the ALPR system. Historical detections placed the suspect vehicle in the desert where the victim was assaulted and left behind, along with other areas where the victim reported they had driven before the assault. The ALPR data was critical in the arrest of this violent attacker.

Fatal Hit-and-Run Traffic Accident

ALPR was used to identify the suspect vehicle that left the scene of a fatal traffic accident after hitting two people. The make and model of the vehicle were identified but not the license plate. The license plate and other supporting evidence were discovered by leveraging the ALPR system. After the crime occurred, ALPR detection records showed significant damage to the suspect vehicle.

2646

Kidnapping

A male subject attempted to grab a female in a business parking lot. Video surveillance captured the subject and his vehicle. Detectives used video footage to determine the suspect vehicle's make, model, and year range. A query of the ALPR system provided sufficient information to confirm the suspect vehicle and registration. The male was later identified. A records check revealed he had two prior arrests for sexual assaults. He was later located and arrested for the crime of kidnapping.

Arson

A subject set fire to the sign and lawn outside an FBI office building. Surveillance footage showed a gold Chevy Tahoe with distinctive damage to the passenger and rear sides of the vehicle. The license plate number was not visible. Analysts searched more than 6,000 images in the ALPR database, looking for Chevrolet SUVs similar to the one in the surveillance footage. After searching the ALPR database, analysts found a vehicle with matching damage, identified the registered owner, then disseminated a bulletin for officers to locate the vehicle. Initially, officers could not locate the registered owner, who was transient. A few days later, a patrol officer spotted the vehicle based on the bulletin and detained the suspect. The suspect was positively identified and linked to the original arson and another one in a different part of the state. Less than one month later, the suspect accepted the criminal prosecution agreement offered by the prosecutors.

2647

Appendix B – Myths and Misconceptions

A review of case law provides a snapshot of the legalities supporting the use of ALPR technology. In contrast, some misinformation exists on the use of ALPR technology by law enforcement. Therefore, reviewing and understanding the myths and misconceptions about ALPR in law enforcement is essential.

MYTH

ALPR detections contain private, personally identifying information.

REALITY

ALPRs are designed to capture three details when a vehicle passes through their view: a photograph of the vehicle, the characters on the license plate of the vehicle, and the location, date, and time when the vehicle passes the ALPR.

Publicly-owned ALPR systems read the license plates of vehicles on public roadways and capture information that is generally not considered private. For example, if an individual were to stand by the side of a public road and take a picture of every vehicle that passed them, write down its plate number, and record the date and time, they would be within their legal rights to do so. Likewise, a person could place a camera on their property facing a public throughway and capture the same information an ALPR does. In *U.S. v. Ellison (2006)*, the Court explained that not only is there no privacy interest in a license plate number, but a subsequent entry into a computer system to retrieve other non-private information does not constitute a search.[3] By states mandating each vehicle operating on the roadway publicly display a license plate and even illuminate it at night, the expectation is for the license plate to be read at any time while on a public roadway.

An ALPR system does not automatically capture or record restricted information contained in an individual's motor vehicle records, such as their name, address, phone number, Social Security Number, driver identification number, etc. *The Driver's Privacy Protection Act of 1994* requires all states to protect this personal information ensuring ALPR reads are anonymous until additional steps are taken to access separate statutorily regulated databases. Therefore, when a law enforcement officer needs to access motor vehicle records based on data captured by an ALPR, they would need to perform the same manual processes to retrieve this information as they would in other investigative circumstances. Additionally, adequate policies limit access to ALPR data by requiring justification for the review of individual ALPR records. This effectively ensures that most ALPR-captured data is never even accessed before it is purged.

Therefore, retrieving non-public information based on ALPR data requires law enforcement to adhere not only to the policies and laws regarding the ALPR data but also to the policies and laws for accessing the restricted databases housing driver's license and vehicle information. In summary, ALPR systems do not grant expanded access to any non-public records databases, nor do they circumvent the auditing processes that are in place to ensure restricted data is accessed only for official use and as permitted by law.

3 United States v. Ellison, 462 F.3d 557, 561, United States Supreme Court. (6th Cir. 2006). https://caselaw.findlaw.com/la-court-of-appeal/1717448.html

MYTH

ALPR technology is a form of mass surveillance.

REALITY

Guided by proper policy and processes, ALPRs are effective tools for law enforcement to narrow the focus of investigations and limit negative collateral impacts when policing high-crime areas.

A scenario most major city police departments are familiar with is as follows: A motorist is stopped by police only to later be released and sent on their way in a case of mistaken vehicle identity. Their misfortune was caused by driving a vehicle matching the general description of one recently broadcasted of a suspect vehicle in a violent crime. Though the detention is usually short-lived, the trauma it causes may not be. This type of "wrong place, wrong time" scenario is most likely to occur when non-specific or incorrect information is relayed to officers during an in-progress incident. Even a single negative experience like this can spread quickly throughout a community, jeopardizing efforts to build trust. Unfortunately, these scenarios most commonly affect residents in neighborhoods disproportionately impacted by violent crime and gun violence. The use of ALPRs can help mitigate these occurrences.

ALPRs provide an additional mechanism to corroborate or refute witness accounts of suspect vehicles. This helps narrow the focus of law enforcement when canvassing and provides officers with the increased ability to bypass lookalike vehicles and only interact with the cars that truly contain the distinct characteristics of the vehicle suspected in the crime.

A common talking point designed to instill fear in ALPRs technology is that they "could" be used to track people involved in first amendment protected activities. The purpose of robust agency policy is to restrict use to legally permissible actions and ensure accountability if rules are broken. It must be noted that the same policies and laws governing law enforcement's actions without technology still apply when using technology. In fact, the audit trails in technology ensure that a hindsight review of any actions taken is afforded an even more detailed perspective than the actions taken without records produced by technology.

Appendix C – State-Level Laws and Regulations

At least 16 states have statutes regarding the use of ALPR or the retention of data collected by ALPR technology. This information was derived from a database maintained by the National Conference of State Legislatures.[4] The states and their laws are as follows:

Arkansas-Ark. Code §§ 12-12-1801 to 12-12-1808

Prohibits use of ALPRs by individuals, partnerships, companies, associations or state agencies. Provides exceptions for limited use by law enforcement, by parking enforcement entities or for controlling access to secure areas. Prohibits data from being preserved for more than 150 days.

California-Calif. Veh. Code § 2413

Provides that the California Highway Patrol (CHP) may retain data from a license plate reader for no more than 60 days, unless the data is being used as evidence in felony cases. Prohibits selling or making available ALPR data to non-law enforcement officers or agencies. Requires CHP to report to the legislature how ALPR data is being used.

California-Calif. Civil Code §§ 1798.29, 1798.90.5

Establishes regulations on the privacy and usage of automatic license plate recognition (ALPR) data and expands the meaning of "personal information" to include information or data collected through the use or operation of an ALPR system. Imposes privacy protection requirements on entities that use ALPR information, as defined; prohibit public agencies from selling or sharing ALPR information, except to another public agency, as specified; and require operators of ALPR systems to use that information only for authorized purposes.

Colorado-Colo. Rev. Stat. § 24-72-113

Requires that video or still images obtained by passive surveillance by governmental entities, such as images from monitoring cameras, must be destroyed within three years after the recording of the images. Specifies that the custodian of a passive surveillance record may only access the record beyond the first anniversary after the date of creation of the record if there has been a notice of claim filed, or an accident or other specific incident that may cause the passive surveillance record to become evidence in any civil, labor, administrative, or felony criminal proceeding. Creates exceptions allowing retention of passive surveillance records of any correctional facility, local jail, or private contract prison and passive surveillance records made or maintained as required under federal law.

Florida-Fla. Stat. § 316.0777

Creates a public records exemption for certain images and data obtained through the use of an automated license plate recognition system and personal identifying information of an individual in data generated from such images. Provides that images and data containing personal information obtained from automated license plate recognition systems are confidential. Allows for disclosure to criminal justice agencies and to individuals to whom the license plate is registered in certain circumstances.

Georgia-Ga. Code § 35-1-22

License plate data may be collected and accessed only for a law enforcement purpose. The data must be destroyed no later than 30 months after it was originally collected unless the data are the subject matter of a toll violation or for a law enforcement purpose. Allows sharing of captured license plate data among law enforcement agencies. Law enforcement agencies deploying an automated license plate recognition system must maintain policies for the use and operation of the system, including but not limited to policies for the training of law enforcement officers in the use of captured license plate data. License plate data collected by a law enforcement agency is not subject to public disclosure.

4 Automated License Plate Readers: State Statutes," National Conference of State Legislatures. https://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx

2650

Maine-29-A M.R.S.A. § 2117-A(2)

Prohibits the use of automatic license plate recognition systems except for certain public safety purposes. Provides that data collected is confidential and may be used only for law enforcement purposes. Data collected may not be stored more than 21 days.

Maryland-Md. Public Safety Code § 3-509

Specifies the procedures and protocols that a law enforcement agency must follow in connection with the operation of an "automatic license plate reader system" and "captured plate data." Requires the State Police to adopt procedures to address who has access to the data and training for those individuals and to create an audit process. Provides that data gathered by an automatic license plate reader system are not subject to disclosure under the Public Information Act.

Minnesota- Minn. Stat. §§ 13.82,13.824, 626.8472

Relates to data practices; classifies data and provides procedures related to automated license plate readers; provides the data that may be collected by such readers; relates to requirements for the sharing of such data among law enforcement agencies; requires the maintenance of a public log recording the uses of such data; requires related records maintenance and the auditing of such records; requires written procedures governing access to the data; requires certain notification when setting up readers.

Montana-Mont. Code Ann. §§ 46-5-117 to -119

Prohibits the use of license plate readers by an agency or employee of the state or any subdivision of the state on any public highway. Provides exceptions for specific agencies or purposes, such as state or local law enforcement, if specified requirements are met. Except as provided, license plate data captured by law enforcement may not be preserved for more than 90 days after the date that the data is captured.

Nebraska- Neb. Rev. Stat. § 60-3201 to 3209

Requires any governmental entity that uses an automatic license plate reader (ALPR) system to adopt a policy governing use of the system. Governmental entities also must adopt a privacy policy to ensure that captured plate data is not shared in violation of this act or any other law. The policies must be posted on the internet or at the entity's main office. Requires annual reports to the Nebraska Commission on Law Enforcement and Criminal Justice on ALPR practices and usage. Provides that captured plate data is not considered a public record.

New Hampshire-N.H. Rev. Stat. Ann. §§ 261.75-b, 236.130

Restricts the use of automated license plate readers to local, county and state law enforcement officers, who shall only use the devices subject to specified conditions and limitations and for specified purposes. Provides that records of number plates read shall not be recorded or transmitted anywhere and shall be purged from the system within 3 minutes of their capture, unless the number resulted in an arrest, a citation or protective custody or identified a vehicle that was the subject of a missing or wanted person broadcast.

North Carolina-N.C. Gen. Stat. §§ 20-183.30 to .32

Requires state or local law enforcement agencies to adopt a written policy governing the use of an ALPR system that addresses databases used to compare data obtained by the system, data retention and sharing of data with other law enforcement agencies, system operator training, supervision of system use, and data security and access. Requires audits and reports of system use and effectiveness. Limits retention of ALPR data to no more than 90 days, except in specified circumstances. Provides that data obtained by the system is confidential and not a public record.

2651

Oklahoma-Okla. Stat. §§ 47-4-606.1

Provides that participating law enforcement agencies may use automatic license plate reader systems to access and collect data for the investigation, detection, analysis or enforcement of the state's compulsory insurance law. States that data collected under the program may not be used by any individual or agency for purposes other than enforcement of the compulsory insurance law, prohibits sale of the data under the program, and provides that data is exempt from the Oklahoma Open Records Act, except when retained as evidence of a violation of the compulsory insurance law. These provisions do not prohibit the use of any other automated license plate reader system by an individual or private legal entity for lawful purposes.

Tennessee-Tenn. Code §§ 55-10-302, 10-7-504(a)

Provides that any captured automatic license plate data collected by a government entity may not be stored for more than 90 days unless they are part of an ongoing investigation, and in that case provides for data to be destroyed after the conclusion of the investigation. Captured plate data from automatic license plate reader systems must be treated as confidential and shall not be open for inspection by members of the public.

Utah-Utah Code §§ 41-6a-2001 to -2005

Provides that a governmental entity may not use an automatic license plate reader system except for specified uses, such as by law enforcement agencies for the purpose of protecting public safety or conducting criminal investigations and by other government entities for limited other purposes. Provides that captured plate data are a protected record under the Government Records Access and Management Act, if the captured plate data are maintained by a governmental entity. Provides that captured plate data may only be shared for specified purposes, may only be preserved for a certain time and may only be disclosed pursuant to specific circumstances such as a disclosure order or a warrant. Government entities may not use privately held captured plate data without a warrant or court order, unless the private provider retains captured plate data for 30 days or fewer. Allows an institution of higher education to use automatic license plate readers under certain circumstances.

Vermont- 23 V.S.A. §§ 1607, 1608

Requires a law enforcement officer to be certified in the use of an automated license plate reader to operate such a system. Provides that active system data may only be accessed by an officer with a legitimate law enforcement purpose for the data. A legitimate purpose includes a person's defense against certain charges and does not include enforcement of parking or traffic violations other than commercial motor vehicle violations. Limits retention and access to information gathered through the use of an ALPR system. Requires the Department of Public Safety to adopt rules to implement the law. Requires the Auditor of Accounts to examine requests for data to determine whether the request and the release complied with the law.

2652

Appendix D – CJIS Security Policy

Agencies that wish to use the CJIS Security Policy to assess the security practices of a service provider that will be handling ALPR data should consider the following sections:

- Private Contractor User Agreements and FBI-CJIS Security Addendum [5.1.5]: Private contractors who perform criminal justice functions for a Criminal Justice Agency (CJA) shall be permitted to access CJI pursuant to an agreement between the CJA and the contractor that incorporates the FBI-CJIS Security Addendum approved by the Director of the FBI.
- Agency User Agreements [5.1.1.6]: Fingerprint-based background checks and written agreement with the agency when required.
- Secondary Dissemination [5.1.3]: If data is released to another authorized agency and not part of a primary information exchange agreement, this shall be logged.
- Security Awareness Training [5.2]: All personnel with access to CJI (Criminal Justice Information) shall receive security awareness training within six months of assignment, and biennially thereafter.
- Security Training Records [5.2.3]: Records of security awareness training shall be kept current and maintained by a Security Officer (CSO).
- Reporting Structure and Responsibilities [5.3.1.1]: Establishment of a primary Point of Contact (POC) for CJIS incident handling and response.
- Events [5.4.1.1]: Description of the events that must be logged within the system.
- Audit Monitoring, Analysis and Reporting 5.4.3]: Responsibility for review and analysis of audit records, at a minimum of once a week, to look for inappropriate or unusual activity.
- Audit Record Retention [5.4.6]: The agency shall retain audit records for at least one year.
- Least Privilege [5.5.2.1]: The agency shall approve individual access privileges and enforce the most restrictive set of rights and privileges needed by users for the performance of specified tasks. Logs maintain access privilege changes for a minimum of one year or at least equal to the agency's record retention policy, whichever is greater.
- Access Control Mechanisms 5.5.2.4]: One or more of the following must be employed: access control lists (users, groups, machines), resource restrictions (permission sets), encryption and strong key management, application-level access control.
- Unsuccessful Login Attempts [5.5.3]: CJIS Security Policy requires that after five consecutive invalid attempts, the account shall be locked out for a minimum of 10 minutes.
- System Use Notification [5.5.4]: The system shall allow a notification message to be displayed to let users know a) they are accessing a restricted system, b) usage is monitored, recorded and subject to audit, c) unauthorized use is prohibited and may result in penalties, and d) use of the system indicated consent to monitoring.
- Session Lock [5.5.5]: CJIS Security Policy requires that the system shall prevent access via a session lock after a minimum of 30 minutes of inactivity.
- Remote Access [5.6]: Rules for monitoring and controlling remote access via the internet.
- Use of Originating Agency Identifiers in Transactions and Information Exchanges [5.6.1.1]: An FBI-issued ORI number shall be assigned at the agency level and attached to all activities by the agency's users.
- Password [5.6.2.1.1]: Requirements and standards for passwords.
- Personal Identification Numbers [5.6.2.1.2]: Best Practices on PIN use.
- Advanced Authentication [5.6.2.2]: Advanced Authentication requirements.
- Identifier Management [5.6.3]: Requirements of agencies to manage user identifiers.
- Network Diagram [5.7.1.2]: Requirements for a network topological diagram.

- Media Protection [5.8]: Requirements for security and protection of electronic and physical media.
- Physical Protection [5.9]: Requirements for physical security and access controls around all hardware, software and media.
- System and Communication Protection and Information Integrity [5.10]: Prevent CJI from being transmitted unencrypted across the public network.
- Boundary Protection [5.10.1.1]: Ensure that failure of boundary protection mechanisms do not result in unauthorized release of information.
- Encryption [5.10.1.2]: Minimum of 128 bit encryption when CJI data is transmitted beyond the physical security boundary.
- Intrusion Detection Tools and Techniques [5.10.1.3]: Requirements for intrusion detection tools.
- Cloud Computing [5.10.1.5 and Appendix G.3]: Recommendations for use of cloud computing and assessment of cloud computing service providers.
- Partitioning and Virtualization [5.10.3]: Requirements for partitioning of data and virtualization of resources.
- Patch Management [5.10.4.1]: Requirements for management of software patches.
- Malicious Code Protection [5.10.4.2]: Virus Protection requirements.
- Spam and Spyware Protection [5.10.4.3]: Spam and Spyware Protection requirements.
- Security Alerts and Advisories [5.10.4.4]: Guidance for alerts and advisories.
- Personnel Security [5.12]: Fingerprint-based background checks and rules based on findings.
- Personnel Termination [5.12.2]: Terminated employees shall immediately have access revoked.
- Personnel Sanctions[5.12.3]: Process for employees failing to comply with security policies.
- Mobile Devices [5.13]: Where appropriate, the technology partner must support the agency's mobile device practices (patch management, etc.)

2654

Appendix E – ALPR Audit and Transparency Report Template

The following template provides a rudimentary example of the details and considerations in providing a published report about the performance and effectiveness of an ALPR program.

Automated License Plate Reader Program
Annual Transparency Report

Introduction

The introduction should provide context and background as to what the report is addressing. The introduction defines the specific objectives and purpose of the report. It indicates any problems that may exist and provides answers to problems explored. Finally, the introduction will preview the report and outline the report structure.

Discussion

This is the main body of the report, and it has two primary purposes. The first is to share and explain the conclusions. The second is to justify any recommendations that may be made in the report.

Specific data points that may be considered:

- Number of detections
- Number of hotplate hits
- Number of queries conducted by users
- Number of arrests directly related to ALPR
- Number of user-generated hotplates
- Breakdown of hotplate hit types
- Year-over-year analysis and trends

Conclusion

This section should relate to the information shared in the report. It should be specific to the objectives of the report. It may also address any issues that may be interpreted from the information shared. The conclusion should be brief, logical, and specific.

Recommendations

Recommendations shared should point to future action that can be completed. Recommendations should be feasible, action-oriented and arranged in order of importance.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Legal Updates

Melissa Johnsen
Deputy Chief, Appeals & Training Bureau

February 8, 2023

Agenda

- 9:30-10:00 Legal Updates
- 10:00-10:55 Search Warrant Process
- 11:00-12:00 Drafting the Affidavit
- 12:00-12:45 Lunch
- 12:45-1:45 Legal Processes for Obtaining Information from Cell Phone & Internet Service Providers
- 1:55-2:55 Search Warrants for Digital Storage Devices & Evidence
- 3:05-4:00 Special Considerations for Digital Device Searches & Warrants

Search Warrants for Blood: Moreau & Bohigian

- Scenario: Defendant is in the hospital following a car crash -- either under arrest or not -- and medical personnel has withdrawn his blood for treatment purposes
- Can police get a warrant to seize the blood and test it themselves?
- Answer: Yes, but the BAC results will not be admissible in a straight OUI prosecution without the defendant's consent
- CW v. Moreau, 490 Mass. 387 (2022): under c. 90 § 24(1)(e), police need the defendant's consent to test blood already drawn by the hospital for the results of a blood alcohol analysis to be admitted in straight OUI prosecution under (1)(a)

Search Warrants for Blood: Moreau & Bohigian

- NOTE: consent requirement of § 24(1)(e) appears to only apply to straight OUI prosecutions under (1)(a), NOT OUI-SBI, OUI-MVH, OUI-Drugs, or Neg Op – results still admissible in those prosecutions (no appellate decision yet)

- Police should still obtain a preservation order and ultimately a warrant to seize the blood and test it – particularly if there are victims involved
  - Charging decision may not be finalized at this juncture
  - Police will likely be obtaining search warrant for medical records in any event

- Police may still attempt to obtain consent, particularly if they are certain that defendant will only be charged with straight OUI-Liquor
  - defendant's license will be suspended for 180+ days if he refuses and is under arrest

Search Warrants for Blood: Moreau & Bohigian

- Scenario: Blood has not been previously drawn by the hospital
- Can the police get a warrant to draw the defendant's blood?
- Answer: No, the police cannot force the defendant to undergo a blood draw to analyze its alcohol content against his will, even if they have obtained a search warrant
- § 24(1)(f)(1) & CW v. Bohigian, 486 Mass. 209, 214 (2020)
- if the police have requested that the defendant submit to a blood draw and he refuses, nothing more can be done other than suspending his license if he is under arrest
- This applies to all OUI-Liquor-related prosecutions (but appears not to apply to OUI-Drugs -- no appellate decision yet)

Juvenile Arrest & Detention

- When a juvenile is arrested, the arresting officer must promptly notify the parent/guardian -- before the juvenile is booked if possible

- In general, a juvenile should only be held at the police station for as long as it takes to notify the parent and to complete the identification & booking process

- Once the booking process is completed, the following should occur:
  - *If the Juvenile Court is in session,* the juvenile should be transported to court for his/her initial appearance
  - *If the Juvenile Court is not in session*, the juvenile should either be:
    - Released to his/her parent, or
    - Transported to the Overnight Arrest Program

Juvenile Arrest & Detention

Where booking is completed <u>while the Juvenile Court is in session</u>:

- c. 119, § 66: child < 18 cannot be detained at station pending arraignment unless court is not in session (§ 67)
- In general, this means that <u>during court hours</u>, juvenile must be transported to Juvenile Court for his/her initial appearance right after booking
- BUT if parent/guardian is present and <u>both</u> juvenile and parent are advised of requirement of prompt arraignment, police may ask juvenile and parent if juvenile would submit to interview prior to being transported to court
- If both juvenile and parent agree to delay transport to court to be interviewed, then prompt arraignment waiver <u>and</u> *Miranda* waiver should be executed
- Once both parent and juvenile indicate that they understand rights, police should inform parent that opportunity is being furnished for them to confer about juvenile's rights, and then leave them alone
- If interview ends after court is closed, juvenile should be released to parent upon written promise that parent will ensure juvenile's appearance in court
- If release is not appropriate, police should ensure interview ends in time to transport juvenile to court
- If juvenile declines to be interviewed, he/she must be brought to court for his/her initial appearance as soon as is reasonably possible

Juvenile Arrest & Detention

Where booking is completed <u>while the Juvenile Court is not in session</u>:

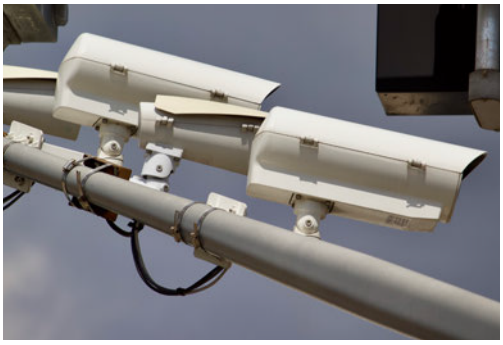
- § 67: police must immediately notify juvenile's parent/guardian when juvenile is arrested and court is not in session
- Pending notification of parent, juvenile is detained in DYS-approved facility separate from adults
- The officer-in-charge determines whether juvenile should be released to parent (exception: juvenile **12 or 13 YO** <u>must</u> be released to parent)
- If release is appropriate, juvenile may be released to parent *upon the parent's written promise that they will ensure juvenile's presence in court*
- If the parent is present, police may ask juvenile and parent if juvenile would submit to interview prior to being released to parent
- If both juvenile and parent agree to be interviewed, *Miranda* warnings should be given to both, and officer should ensure that both understand rights
- Once both parent and juvenile indicate that they understand rights, police should inform parent that opportunity is being furnished for them to confer about juvenile's rights, and then leave them alone
- Juvenile may be briefly detained to secure any biological/chemical evidence as long as there is probable cause to seize such evidence and exigent circumstances dictate that it must be seized without delay
    - Police should document the reasons for the exigency

2697

AAMVA

American Association of
Motor Vehicle Administrators

technology
POLICY security
Safety training
REVENUE Data
ACCURACY



License Plate Reader Program
Best Practices Guide





October 2021

LAW ENFORCEMENT STANDING COMMITTEE
VEHICLE STANDING COMMITTEE

2021 © Copyright All Rights Reserved
American Association of Motor Vehicle Administrators

Cover photo credits: © iStockphoto.com

Contents

Executive Summary 2

Chapter 1 Introduction 3

Chapter 2 License Plate History 5

Chapter 3 License Plate Reader Fundamentals 9

Chapter 4 License Plate Reader Benefits 17

Chapter 5 License Plate Readers as a Tool to Improve Toll, Commercial Motor Vehicle, and Border Operations 20

Chapter 6 License Plate Reader Program Best Practices for Law Enforcement 24

Chapter 7 License Plate Reader Success Stories 28

Appendix A Significant License Plate Reader Court Cases and Applicable Federal Statutes 30

Appendix B Additional License Plate Reader Resources 34

Appendix C Sample License Plate Reader Policies 35

Appendix D AAMVA License Plate Reader Working Group Roster 49

Executive Summary

Since their inception more than a century ago, license plates have primarily been used to display information for fast and accurate identification of motor vehicles and to demonstrate compliance with motor vehicle registration laws.

In support of their highway and public safety missions, License Plate Readers (LPRs) provide law enforcement with the ability to check license plates against various databases. Tolling and parking enforcement authorities also rely on LPR technology for the collection of tolls and enforcing parking regulations.

Law enforcement agencies can build meaningful LPR system policies that respect individuals' privacy rights while providing authorized users with the information necessary to ensure the public's safety.

More than a decade ago, it was recognized that inconsistent business rules used by license plate issuing authorities were resulting in alarmingly high "misreads," diminishing law enforcement's ability to identify and apprehend suspected criminals and terrorists, recover stolen vehicles, and assist people in need of assistance. Similarly, tolling and parking authorities are hampered in their revenue collection mandates that are critical to maintaining infrastructure and ensuring parking regulations are not flouted. In addition, license plate misreads hamper Customs and Border Protection's ability to correctly identify vehicles crossing international borders.

In response to this issue, in 2012, AAMVA published a *Best Practices Guide for Improving Automated License Plate Reader Effectiveness Through Uniform License Plate Design & Manufacture*. At the time, AAMVA did not have a License Plate Standard. Since that time, AAMVA has published a License Plate Standard (2016) and a License Plate Standard, Edition 2 (2020).

In 2020, the AAMVA Law Enforcement and Vehicle Standing Committees determined the 2012 LPR document should be retained but with content now covered in the License Plate Standard removed and the remaining material updated and added to as appropriate. This guide has been renamed *License Plate Reader Program Best Practices Guide* and has been refocused on best practices in the administration of LPR Programs for state and provincial law enforcement, although much of the content is applicable to tolling and parking enforcement authorities alike.

Chapter 1 Introduction

License Plate Readers (LPRs) are an effective law enforcement and traffic safety tool and are critical to government entities—such as tolling and parking enforcement authorities—who use the technology to enforce the law and collect revenue. LPRs enhance public safety and security by providing law enforcement the ability to check license plates against databases such as the National Crime Information Center. The databases searched are at the discretion of each law enforcement agency using LPR technology.

Federal, state, local, and tribal public safety agencies rely on accurate and timely license plate information to effectively and efficiently perform the multiple tasks required in the performance of their duties. Information is available in multiple formats, including hot lists (e.g., stolen vehicle), Be On the Look Out (BOLO), Attempt to Locate (ATL), officer safety information, AMBER Alerts for at-risk children, SILVER Alerts for at-risk adults, and more. Much of this information can be, and often is, associated with a vehicle's license plate. The ability of LPRs to quickly and accurately scan thousands of license plates is critical to the men and women of law enforcement who contact hundreds of thousands of people throughout the U.S. and Canada every day, as well as to Customs and Border Protection officers and agents monitoring international ports of entry. When LPRs misread license plates, law enforcement is hampered in its mission to protect and to serve, and government entities lose revenue from uncollected tolls.

The International Association of Chiefs of Police conducted a 2021 survey of police agencies across the U.S. about their use of LPR systems. More than 1,200 agencies responded to the survey measuring LPR use, policy considerations, data retention and management, and more.[1]

Among all respondents:

- **40%** reported currently using LPR systems in their departments.
- Cost was the biggest barrier to LPR use.
- Larger agencies were more likely to use LPR systems than smaller agencies were.
- Mobile units were the most common form of LPR system used.

Among agencies using LPR:

- **75%** owned their own LPR system. Others contracted use of their LPR system or leveraged another agency's LPR system.
- **63%** shared their system with another agency, and **84%** shared their LPR data with other agencies.
- **64%** reported full control of the data in their LPR system.
- **44%** of the agencies using LPR stored their data on the cloud, and **43%** stored their data on agency servers or other government resources.

A study conducted by the Police Executive Research Forum[2] concluded that LPRs increased license plate reads by a factor of more than eight. What the study did not, and could not reveal, is the number of hits "missed" because of license plate misreads. Regardless of the misread rate in a particular jurisdiction, there

1 As of this printing, these represent preliminary estimates only.

2 Combating Auto Theft in Arizona: A Randomized Experiment with License Plate Recognition Technology: Police Executive Research Forum, December 2011.

is no refuting that misreads occur. And when they do, the potential exists to miss opportunities to arrest a suspected criminal or terrorist, to recover a stolen vehicle, or to collect toll revenue.

A completely effective "ecosystem" is needed to ensure as close to 100% as possible accurate license plate read rate is achieved by LPRs. Multiple stakeholders share the responsibility for maintenance of the ecosystem. Motor vehicle agencies having license plate design and manufacture administration oversight responsibility should ensure their issued license plates align with the AAMVA License Plate Standard (see Appendix B). LPR manufacturers have a responsibility to develop and implement state of the art technology to accurately read the multi-variant license plates that exist. Law enforcement and other government entities using LPR are responsible for ensuring they have policies and training that align with the most current best practices available.

AAMVA published a *Best Practices Guide for Improving Automated License Plate Reader Effectiveness Through Uniform License Plate Design & Manufacture*. At the time, AAMVA did not have a License Plate Standard. Since that time, AAMVA has published a License Plate Standard (2016) and a License Plate Standard, Edition 2 (2020) (see Appendix B).

This LPR Program Best Practices document, combined with the AAMVA License Plate Standard, Edition 2; License Plate Policy Statements; and License Plate Verification Program all serve to assist jurisdictions in shaping of jurisdiction laws and regulations and operational policies ensuring license plate readability and integrity.

In 2020, the AAMVA Law Enforcement and Vehicle Standing Committees determined the 2012 document should be retained but with content now covered in the License Plate Standard removed and the remaining material updated and added to as appropriate. This guide has been renamed *License Plate Reader Program Best Practices Guide* and has been refocused on best practices in the administration of LPR Programs for state and provincial law enforcement, although much of the content is applicable to tolling parking enforcement authorities alike.

AAMVA also has four policy statements addressing license plates (see Appendix B).

In 2020, AAMVA launched the License Plate Verification Program (LPVP). The LPVP allows jurisdictions to submit up to four license plates per fiscal year for examination and comparison with the AAMVA License Plate Standard, at no cost to the jurisdiction. The examination is conducted by an independent third-party laboratory under contract with AAMVA. A written report is provided to the submitting jurisdiction outlining areas where their license plate(s) do, and do not, align with the License Plate Standard. The report identifies for jurisdictions areas for potential improvement in the readability of their license plates.

Chapter 2 License Plate History

Introduction

Since their inception more than a century ago, license plates have primarily been used to display information for fast and accurate identification of motor vehicles and to demonstrate compliance with motor vehicle registration laws. The advancement of manufacturing technology has resulted in more colorful and detailed graphics on plates, which can be used to promote a jurisdiction or organization but at times have created an identification challenge for law enforcement and a readability challenge for camera technology. Most jurisdictions now have numerous plate types and designs available to the public.

Hand-Made, Horse-Drawn

The first record of a registration plate in the U.S. was in Philadelphia, Pennsylvania, in the 1850s. Even then, legibility of plates was a concern, and horse-drawn vehicles required registration to be identified with numbers "not less than four inches high." Among other things, these numbers provided a means of identification when reporting an incident involving inappropriate or reckless driving. Today, only the state of Indiana still requires a license plate on a horse-drawn carriage.

The construction of these early registration plates was left to the innovation of the vehicle owner; wood, brass, or other metals affixed to leather backings were common materials used. During the next 50 years, many cities required registration, and they frequently required payment of a modest registration fee.

Plate Production and Issuance

In the early 1900s with the advent of motorized vehicles, jurisdictions took responsibility for registration and standardization of plate issuance.

In 1901, New York became the first state to require license numbers on motor vehicles. In 1903, Massachusetts was the first state to issue a standard statewide plate. Others soon followed, but issuance of plates remained inconsistent.

California also began requiring plates in 1903 but did not produce them; the Automobile Club of Southern California (an early AAA organization) issued license plates—called mouse ears—to members for $1.00. The state assumed this responsibility in 1910.

On March 22, 1905, the Maine senate debated House Document 552, which required automobiles to be registered and plates to be issued. A senator argued in favor of the plate by stating: "The point upon this bill comes is upon the matter of registration. What does it mean? The matter of registration does not prevent the violation of the law, but the matter of registration, and the law compelling the carrying in a conspicuous position, of a certain number, which leads to the registration and which may lead to the detection or recognition of a violation of the law, is all that registration can amount to as to guarding the safety of the public against accidents from automobiles."

As the debate continued, another senator voiced his support for the display of a number on automobiles so that the operator could be identified when it frightened a horse. In part he stated, "I do not own

an automobile, and do not ever expect to. I do own a cheap horse and have a wife and three girls that drive it. What is the result now? They do not dare to go out. I have a safe horse, but when one of those reckless fellows comes along (*in an automobile*), they are likely to get tipped out, as many have in the State of Maine."

The debate continued, the bill passed and became public law Chapter 147. It required the Secretary of State to license operators, to register automobiles and motorcycles, and to issue plates. The law also required the Secretary of State to "furnish the applicant two enameled iron plates containing the word 'Maine' and the number of the registration in Arabic numerals not less than four inches in height. The number plates must be attached to the front and back of the automobile and one number plate must be attached to the back of motorcycles."



Maine plate, 1905 to 1911. The width changed based on the number of characters on the plate.



Starting in 1903, "mouse ear" plates were sold for $1 by the Automobile Club of Southern California.

By 1915, nearly all jurisdictions issued license plates on an annual basis and charged a registration fee that allowed a vehicle to be driven on public roads. Government officials recognized early on that a registration system provided for vehicle identification and a source of transportation revenue. However, license plate design continued down an inconsistent path. It wasn't until 1956 that a standard plate size (12" x 6") was introduced at the request of automobile manufacturers to make it easier to incorporate license plates.

Integrating Safety Concepts

With the rapid increase in the motor vehicle population in the 1920s and 1930s, traffic crashes increased dramatically, leading to the need to improve not only vehicle identification but also vehicle safety. License plates became one means to improve safety by providing a device that improved the night visibility of motor vehicles. The first retro-reflective license plates in the U.S. were issued by New Mexico in 1936.

As retro-reflective technology advanced, fully retro-reflective plates became possible and the first was issued by Connecticut in 1947 followed by Maine in 1949. Delaware followed suit in 1950 followed by Rhode Island and Oregon in 1951.

During the 1950s, relatively new sheeting gave retro-reflective plates their biggest boost. Minnesota had the distinction of being the first state to use the sheeting on automobile license plates.

The effect that retro-reflective plates had on nighttime motor vehicle crashes was dramatic, and it did not go unnoticed. In 1956, the first year of use in Minnesota, deaths caused by automobile crashes in rural areas dropped from 24% to 9%. Urban area fatalities involving parked vehicles decreased from 28% to 7%.

Standards Materialize

Tiny San Marino—the smallest republic in Europe, with an area of only 24 square miles—had the distinction of being the first country on that continent to make reflective license plates mandatory on all 2,500 of its automobiles. In the other hemisphere, the South and Central American countries of Peru and Costa Rica also became pioneers in retro-reflective license plates. In Canada, the provinces of Newfoundland and Alberta led the way. Today, all 50 U.S. states and most other countries in the world use retro-reflective plates.

With the advent of retro-reflective license plates, law enforcement realized a benefit in improved legibility.

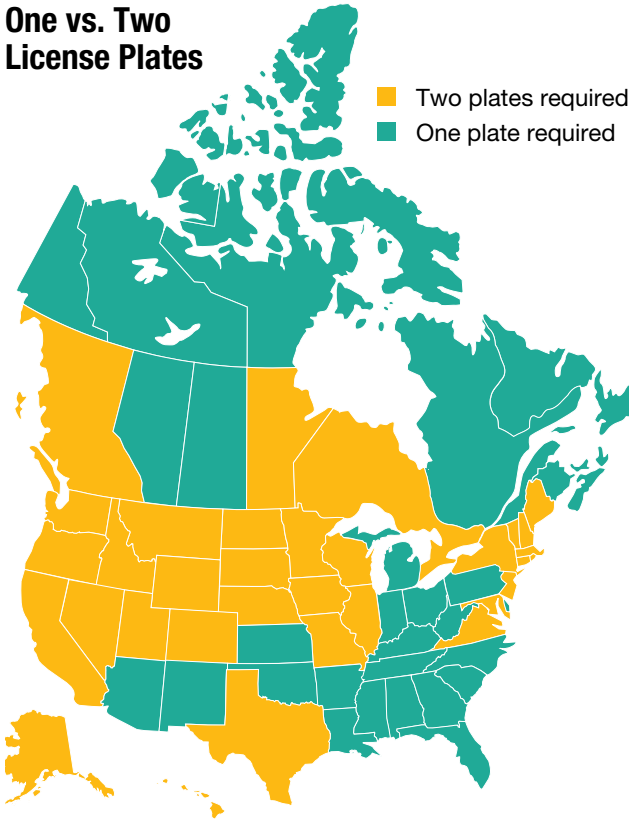
Although one of the original intents of a vehicle registration number was to aid law enforcement, the reality was that non-reflective plates could only be easily read during daylight hours. Retro-reflection provided greatly improved legibility at night, and even today fully retro-reflective plates continue to have strong endorsement from U.S. law enforcement officials, who advocate fully retro-reflective plates on both the front and rear of vehicles for improved safety and law enforcement efficiency.

Although early license plates were often homemade or devised of porcelain, steel became the predominant base material for plates during the first half of the 20th century. Today, aluminum dominates as the material used in license plate manufacture.

After 1945, most states returned to the pre-war practice of requiring two plates per vehicle. Since then some states have moved from two plates to one or vice versa. States typically move to one plate with the intent to save on the cost of the second plate. During the late 1980s, Connecticut was the last state to move from one plate to two plates. Law enforcement effectiveness was cited as the primary reason for the change. The U.S. and Canada are two of a small number of countries that allow one plate. The following chart identifies the North American jurisdictions that require either one or two license plates.

Within the U.S. and Canada, each jurisdiction is responsible for issuing license plates for vehicles registered in their jurisdiction. To create a plate unique and easily recognizable to that jurisdiction, combinations of colors were originally used. Plate background color and colors of the alphanumeric were varied, along with the characters, to create the necessary combinations needed for vehicle classifications and to differentiate plates among the jurisdictions. With increases in vehicle populations and registration classifications, color alone was not enough. Graphic technology became available in the early 1970s that allowed another level of differentiation of license plates. In 1973, Illinois was the first state to use graphics preprinted on the reflective sheeting, for a special plate for disabled veterans. South Dakota quickly followed with the first general issue graphic of Mount Rushmore National Monument. Today all jurisdictions use graphic plate design. When first introduced, graphic design plates were viewed as attractive and as a mechanism to enhance the image of the jurisdiction.

One vs. Two License Plates



Three Canadian jurisdictions require two plates and 10 require one plate. Thirty U.S. States and the District of Columbia require two plates and 20 states require one plate. NOTE: The five U.S. Territories are not included.

However, since the proliferation of graphic plate designs, law enforcement is no longer able to easily recognize the issuing jurisdiction. The widespread use of graphics and colors frequently makes legibility of the plate characters a challenge for law enforcement.

Modern Features, Security, and Function

Until the 1990s, all the U.S. and Canada and most of the rest of the world produced license plates with raised (embossed) alphanumeric characters. In the late

1990s, digital printing technology was introduced, resulting in flat, digitally printed license plates. Today, many states are issuing flat plates. Some jurisdictions issue a combination of embossed and flat plates.

As a result of increasing concern with the use of counterfeit license plates used to perpetrate crimes, security features were added to license plate. These security features allow for easy recognition of fraudulent plates and provides one more obstacle for criminals to overcome.

The following functions of a license plate have been, and continue to be, the most important over the past century:

- Display of information necessary for fast and accurate identification of a motor vehicle and compliance with motor vehicle registration laws
- A validation sticker is issued in most jurisdictions, often rotating the color, to indicate a current and valid registration
- Provide an added margin of visibility and safety by making vehicles more visible

More recently, additional functions of license plates have emerged to

- Provide revenue for highway funds and sponsoring organizations (specialty and vanity plates)
- Use images of plates to improve and increase toll collection, parking fees, and fines
- Provide a way for individuals to express their pride or to promote various causes
- Provide access control to parking, facilities, and gated communities.

Alternative Vehicle License Plates

Two nontraditional license plate technologies have recently emerged: digital license plates and front license plate wraps. These alternative vehicle license plates are intended to replace traditional aluminum or metal license plates.

Digital license plates are reflective but not retro-reflective, creating challenges for law enforcement, tolling authorities, and others that read license plates in all light conditions and rely on License Plate Reader (LPR) technology, which is currently programmed to read retro-reflective license plates.

A license plate wrap is an adhesive license plate applied to a vehicle's bumper. Wraps, where currently authorized for purchase, are only allowed to be applied to the front of a vehicle.

A curved, indented, or otherwise non-flat surface could render the wrap unreadable to LPRs or the human eye.

For a fuller explanation of both the benefits and challenges associated with nontraditional license plates, see the AAMVA License Plate Standard, Edition Two, Chapter 5 – Alternative Vehicle License Plate Displays.

Chapter 3 License Plate Reader Fundamentals

Introduction

This section provides an overview of License Plate Readers (LPRs), the license plate reading process, and key challenges faced by LPR systems.

Typical applications for LPR technology by law enforcement, motor vehicle administrations, and other entities include but are not limited to:

- Law enforcement stolen vehicle and other "hot list" files
- AMBER, BLUE (violent criminal who has killed or injured a law enforcement officer), and SILVER Alerts
- Open road tolling (pay by plate)
- Congestion pricing
- Parking enforcement
- Access control
- Traffic studies
- Automated speed enforcement
- On-street parking enforcement
- Travel or journey time calculations

As the demand for LPR systems expands in both law enforcement and commercial applications, LPR technology continues to evolve. LPR provides cost-efficient approaches in varied environments that include both environmental challenges (e.g., mobile-based platforms, high-speed traffic) and license plate challenges (e.g., introduction of new designs, fonts, and so on across multiple jurisdictions).

The reads from LPR systems, namely the license plate number and in some applications the license plate jurisdiction, are primarily used as input into downstream systems to support the intended application. For example, whereas in open road tolling systems, the license plate number and jurisdiction are used to support the collection of toll revenues, in federal and state law enforcement systems, the license plate number and jurisdiction are used to support law enforcement queries against both large-scale (e.g., National Crime Information Center) and local data sources.

In some applications, manual verification or certification of LPR results is required at some point in the process. To the extent LPR systems can improve and retain a high degree of accuracy, operational costs can be reduced. In some applications, LPR system service-level objectives call for a 95% accuracy rate in correctly identifying both the license plate number and jurisdiction when the license plate is completely visible in the license plate image. The most significant challenge to maximizing license plate read rate accuracy is the ability of LPR system vendors to quickly adapt to the introduction of jurisdictional license plate designs with varying fonts, graphical designs, stacked letters, and so on.

License Plate Reader Systems

LPR systems include deployment of fixed, portable, mobile, and mobile application platforms.

Fixed Platforms

Fixed LPR platforms are permanently mounted on fixed infrastructure such as overhead gantries or roadside bollards. LPR fixed platforms are commonly used in open road tolling, commercial vehicle weigh station operations, and some federal and local law enforcement applications.



Fixed LPR in weigh station operations.



Fixed LPR in Customs and Border Protection inbound.

Portable Platforms

Portable LPR systems can be transported between locations, assembled, operated, and then disassembled. Once deployed, they operate as a fixed platform. Examples include portable trailers, traffic barrels, and other platforms configured with or containing LPR equipment.



Portable department of transportation trailer with LPR.



Speed trailer with LPR.

Mobile Platforms

Mobile LPR systems are defined as any LPR system that is mounted on a vehicle, whether a police car, tow truck, street sweeper, parking enforcement vehicle, and so on. These systems can include one to four camera configurations and are typically mounted on the roof or trunk, or they are custom manufactured.

Typical components of mobile systems include cameras that obtain images of the plate and vehicle, which in turn are passed to a processor mounted in the trunk. The processor locates the license plate in the image and extracts the license plate number. It then compares the textual license plate read against selected data sources and sends the output in the form of an alert to a mobile data terminal (screen) and an operator in the cab. The alert typically contains the name of the data source to which the image was compared such as an expired license or registration system, an infrared (IR) image of the license plate, and a color overview image of the vehicle in question. Data generated from mobile LPR systems can also be stored or transmitted via a back-office software application.



Patrol vehicle roof-mounted LPR.



Parking enforcement roof-mounted LPR.

Mobile LPR Applications (Apps)

Mobile LPR applications are defined as LPR systems that are held and operated by individuals using devices such as barcode readers, ruggedized PDAs, and smart phones that provide other capabilities (e.g., communications, internet access). These technologies provide mobile LPR capabilities and rely on the user to point the imager toward the location of the license plate.



LPR application on a mobile device.

Use of these devices is limited to speed applications typically less than 45 mph and are subject to unique challenges such as shadows, low ambient light, distance or angle to the license plate surface, and non-reflective surfaces. These limits can be overcome using techniques to light or IR illuminators resident in the device. Because IR imagers are not typically available on commercial general-purpose handheld devices, overcoming readability of non-reflective surfaces using a color imager generally requires special Optical Character Recognition (OCR) techniques. The accuracy of these OCR devices is dependent on the specific device and environment in which it is being used.

Handheld platforms are useful because they are easily deployed and can be used in parking enforcement, covert applications, portable checkpoints, and more. Benefits include portability, relatively low cost, and tactical use. The biggest drawback is that when the LPR application is used, it drains the device battery much faster than normal usage.

LPR Camera Technology

Two primary approaches are used to capture images from which the license plate information can be extracted. One approach is to capture a single still image of the license plate at an "optimal" distance from the camera, where the illumination, lens settings, and field of view can all be controlled to yield the best possible images under any ambient lighting and weather conditions. Another approach is to capture multiple images as the vehicle travels through the field of view of the camera. In this approach, near-instantaneous adjustments to the flash, shutter, and gain settings are performed to optimize the license plate image for different environmental conditions.

Monochrome (black and white), color, and IR cameras are used in various solutions. Monochrome cameras tend to yield the best resolution, can work with most types of visible light illumination, and are generally less costly. Color cameras are useful when the color information can be used to improve

the separation between characters and background and for identification of the jurisdiction. Color cameras require white light to produce accurate color information and are of very limited value at night without the use of additional illumination.

IR cameras are tuned to respond to IR illumination. IR cameras tend to be most sensitive at night and tend to be fitted with a band-pass filter designed to block visible light (to limit the effect of headlights and sunlight). This tuned IR illumination is effective at reflecting off the reflective background finish of the plate and not reflecting off the non-reflective characters (or vice versa).

Additional cameras are often used as part of the solution so that both a plate image and a vehicle image can be simultaneously captured to provide context and for investigative purposes. Multiple cameras are also useful when multiple bandwidths of light are used. For example, the fusing of white light and NIR (near-IR) light imagery adds significant information during the OCR and jurisdiction determination.

License Plate Recognition Process

The license plate recognition process begins when a vehicle is detected by an LPR system and ends when an LPR system information has been collected, analyzed, and handed off to backend systems for further processing.

The key steps of the LPR process are to

- Detect the vehicle and/or license plate.
- Locate the license plate in the image(s).
- Extract license plate characters from the background.
- Identify the license plate number.
- Determine the license plate jurisdiction *(optional).*
- Hand off LPR results to backend systems.

The following paragraphs describe each of the LPR steps in detail.

Detecting the Vehicle and/or License Plate

External triggers such as through-beam IR sensors, retro-reflective license plate sensors, ground-based induction loops, laser range sensors, and so on can be used to detect the presence of a vehicle in the field of view of the ALPR system. These types of triggers are primarily used in fixed-platform ALPR systems. Alternatively, the ALPR system detects the presence of a license plate by analyzing the camera's video signal (which may capture up to 60 images per second) and looking for potential license plate candidates. This type of detection is primarily used in mobile platform ALPR systems and can support vehicle speeds up to 140 mph. When the vehicle is detected, the ALPR captures one or more images containing the license plate that will be used to support the subsequent license plate number and jurisdiction determination.

Locating the License Plate in the Image

After one or more images containing a license plate are captured, a "license plate finder" algorithm is used to determine the exact location of the license plate in the image. This may be accomplished by searching for license plate characteristics (e.g., high-contrast objects) or character strings in the image that indicate the presence of a license plate. This process is one of the most difficult steps of the LPR process because the license plate must be located in potentially conflicting images that contain other information that may appear as license plates (e.g., bumper stickers, other writing, contrasting graphic designs). In addition, the type and condition of the license plate (e.g., retro-reflective, non-reflective, license plate frames and covers, license plate orientation) may require the use of special lighting and camera technologies to both locate and present the optimal license plate image to the character recognition algorithms.

As shown in the picture below, LPR cameras can vary flash, shutter, and gain settings to capture multiple images per vehicle over a wide range of ambient and environmental conditions.

Camera Arrangement	Resulting Image with Unchanged Ambient Conditions
Flash Duration = 130 µs Shutter Duration: = 200 µs Gain = 2	
Flash Duration = 390 µs Shutter Duration: = 500 µs Gain = 2	
Flash Duration = 780 µs Shutter Duration: = 1000 µs Gain = 2	

By varying camera settings and controlling illumination, the ability to locate a license plate within an image can be greatly improved. In addition, the 'best' image can also be used to improve the accuracy of the subsequent character extraction and license plate number determination.



License plate that has been located in the larger vehicle image captured by an LPR camera.

Extracting the Characters from the Background (Segmentation)

After the license plate is identified in the images(s), the region around the license plate may be further analyzed to extract the characters from the background. In the following example, pixels making up the candidate region are separated into foreground and background pixels to provide a more suitable candidate image used by the OCR algorithms to translate a character string image into an alphanumeric value that constitutes the license plate number. This is made more difficult when there is little contrast between the license plate number and the plate background.



The segmented or pre-processed license plate image is then passed off to OCR software, where the images are converted to individual alphanumeric characters.

Determining the License Plate Number

Challenge: Poorly designed fonts and variations in fonts themselves, additional symbols, half-height characters, location of registration stickers, license plate frames and covers, and holograms on characters all increase the complexity of OCR algorithms used to determine the alphanumeric characters of a license plate.



In the following example, you can see the software cannot discern whether the first character is a "B" or and "8" and whether the third character is a "6" or a "G."

In the following license plate examples, the ascender and descender of the letter 'Q' takes on different characteristics that may require specifically tuned or trained OCR engines depending on the region or jurisdiction in which the LPR system is deployed. The number '4' in the first license plate compared with the '4' in the second photo below provides another example of inconsistent fonts used between jurisdictions, making the same number look different. Note that the image processing and segmentation steps described must discern the actual license plate number from other alphanumeric information such as vehicle registration tabs and jurisdiction names and logos.





Determining the License Plate Types and Jurisdiction

Some LPR systems can identify the license plate type and the jurisdiction of origin by recognizing key features on the plate such as the jurisdiction logo, background graphics, special symbols, unique character font features, and so on. Other techniques include applying syntax rules and other regionalization rules to provide additional clues to determine the license plate jurisdiction. Use of white light for this process significantly improves the accuracy of jurisdiction identification. Many of the jurisdiction specific features are lost when imaging the license plate in the NIR light spectrum.



Handing Off LPR Results to Backend System

After the license plate number and, in some cases, the jurisdiction, are determined, the information is handed off to backend systems in support of the intended LPR system application. These systems may compare the license plates with watch lists or other law enforcement systems to allow interdiction or other actions to occur in near real time. Sometimes these actions are not for interdiction purposes but merely to allow vehicles to gain access to secure locations, parking garages, and so on.

In some cases, the LPR data—along with supplemental data such as scene and driver images, vehicle location, and date and time stamps—are stored in highly scalable and searchable data sources to support intelligence analysis, bill generation, or other processes that may occur at a later date.

LPR systems are often configured to automatically communicate or transmit all the collected data to a backend data archive or server. Communication methods can include any conventional networking protocols, including cellular, Wi-Fi, hardwire, and thumb drives, all with a variety of security protocols. In many cases, this communication process occurs in the background without any effort from the system user.

After the data have been inserted into the backend data management software, they are immediately available for review and search. These systems are generally web based and can support numerous workstations simultaneously. Often the software solutions used to manage data sources allows information to be queried in a multitude of ways, by location, time, plate number, and so on.

In addition, the image captured and the results generated by the ALPR system can be digitally signed and encrypted to enable a third party to verify that the data was collected at a specific time and location and that no one has tampered with it. This approach also provides for a chain of custody for legal evidence purposes.

Challenges Associated with License Plate Reading

Certain steps of the LPR process present unique challenges that require continuous innovations in hardware and software technologies. A key challenge is the constant introduction of new and varied license plate designs that greatly expands the types of license plates

that LPR systems are required to process. Some of those challenges and the current techniques being applied to address these challenges include the following.

Detecting the Vehicle and/or License Plate

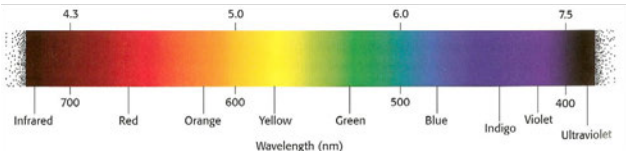
Challenge: LPR systems operate in outdoor environments subject to constantly changing conditions, including lighting, weather, varying vehicle speed and acquisition angles, and varying distances from cameras.

Techniques: LPR camera locations, focal points, illumination controls, and vehicle detection sensors are carefully controlled to help ensure the capture of optimal images used for subsequent license plate location and OCR. Often ALPR cameras are sequencing illumination levels or acquisition parameters to counteract the constantly changing conditions in which they are operating.

Locating the License Plate in the Image(s)

Challenge: Low-contrast license plates, license plate frames and covers, and other noise in the image (e.g., bumper stickers) all impact the ability of license plate detection algorithms to locate the license plate in the larger image captured by the LPR system.

Techniques: Commercial LPR systems typically use a narrow band of IR illumination to light the plate for detection purposes in nearly all weather and lighting conditions. This band ranges from 750 nanometers (nm), which has a visible bright red glow, to 810, 850, 940, and 950 nm. A 950-nm IR illumination is completely invisible to the naked eye.



The purposes in using several bands of IR light are to filter out the effects of background graphics and to highlight the alphanumeric characters for OCR software systems. To help overcome graphic-heavy backgrounds, a spectral analysis can be performed automatically on a plate-by-plate basis to determine which IR illumination is best suited for each plate at the time it is read by the LPR. In general, lower IR bands such as 750 nm handle heavier graphics, and higher IR bands of light are more effective with lower density graphic backgrounds.

Extracting License Plate Characters

Challenge: License plates with conflicting backgrounds or graphics that encroach on the character fields present conditions that make it difficult to recognize specific license plate characters.











Technique: To address these challenges, LPR systems can use different illumination techniques to improve the contrast between characters and background. Also, specialized segmentation algorithms are used to segment the characters from the background. Many LPR systems use neural networks that are trained to find characters correctly in cases of low contrast between characters and background.



In this example, the R could be read as an A and the Q as an O.



The first photo shows a plate with three stacked characters (the AAMVA License Plate Standard calls for no more than two characters to be stacked). The second photo shows appropriate half-height stacked characters. In some jurisdictions, the stacked characters are considered part of the plate number, but in other cases, they are not.



When characters are located too close to the plate's edge, license plate frames can easily prevent the plate number from being read by an LPR.

Chapter 4 License Plate Reader Benefits

Introduction

Prior to the introduction of License Plate Reader (LPR) technology, a law enforcement officer could run a minimal number of plates per shift. LPR technology allows an officer to "read" more than eight times the license plates than officers conducting only manual checks. LPR systems may be used in targeted areas such as crime hot spots, assisting law enforcement in obtaining valuable information of vehicles that may be involved in criminal activity. Moreover, by eliminating the manual check process, not only is officer efficiency increased, but it allows officers to focus more on their surroundings, which improves both officer and public safety.

In studies supported by the National Institute of Justice, research was conducted as to the effectiveness of LPR use for law enforcement patrol and investigations. The first study was conducted in a large suburban jurisdiction in designated hot spots for a period of four months. Officers who used LPR were found to be much more likely to recover stolen vehicles than officers who did not use LPR. The second study examined how LPR could be used for investigations and was focused on a large city with nearly 100 LPRs in fixed locations. After two years, researchers noted 4,000 incidents were documented, including auto theft, missing persons, and homicide cases. LPRs were found to provide information that contributed somewhat to resolving roughly one in five incidents.[1]

Misreads of license plates by LPRs or illegible license plates causing no reads by LPRs do occur.

1 Christopher S. Koper and Cynthia Lum, "Effectiveness of License Plate Readers for Patrol and Investigations," Research in Brief, Police Chief 85, no. 9 (2018): 14–15.

Research conducted by one major toll authority from December 2020 indicated that 9% of toll revenue was lost because of unbillable revenue from misread or illegible license plates.



Gantry mounted LPR technology commonly used for automated toll collection.

When they do occur, the potential for arresting the wrong person, missing an opportunity to arrest a suspected criminal or terrorist, recover a stolen vehicle, or miss toll revenue exists. Research conducted by one major toll authority from December 2020 indicated that 9% of toll revenue was lost because of unbillable revenue from misread or illegible license plates.[2]

Challenges to Law Enforcement

In the past, a law enforcement officer could be familiar with all 50 states' license plates. Today with the proliferation of license plate designs, specialty, and vanity plates—in some cases into the hundreds in a single jurisdiction—it is virtually impossible for instant visual recognition for today's police officer. The issue

2 E470 Public Highway Authority Quarterly Dashboard Report December 31, 2020.

is exacerbated by the introduction of additional new license plate designs each year. Moreover, novelty plates that closely resemble official license plates have added to the difficulty law enforcement contends with in determining plate validity.

A sampling of eight states illustrates the significant growth in the number of license plate designs in circulation in the U.S.

This table represents a sample of the growth in license plate designs:

Jurisdiction	2009	2012	2021
Arizona	52	64	75
California	106	117	167
Maryland	800	935	1,365
Missouri	172	200	269
Montana	152	177	350
Pennsylvania	245	310	582
South Carolina	385	417	429
Texas	225	376	499
8 state totals	2,137	2,596	3,736
% Increase from 2009 to 2021			57%

Officer Safety Benefits

Safety is of paramount concern for any law enforcement officer initiating a "routine" traffic stop. Officers in patrol vehicles that are not equipped with LPR technology may not be as informed about the vehicle and its occupants as those who have the technology.

LPR technology provides the ability to check the vehicle plate number automatically and rapidly against selected databases. License plates are often "flagged" when the owner is associated with certain information (e.g., wanted, attempt to locate, be on the lookout for, stolen car). With LPR technology, officers stopping drivers for sometimes minor traffic offenses can be made aware of this type of information, which allows them to use the appropriate officer safety tactics given the information they have instead of unknowingly walking into a dangerous encounter.

Traffic Safety Benefits

One significant example of a traffic safety benefit involves suspended, *revoked, or otherwise ineligible* drivers. *Across North America, at any given time, approximately 7% of all drivers are suspended, and it is estimated as many as 75% of these people continue to drive.*[1] Moreover, 19% of all fatal crashes involve an unlicensed or suspended driver. These drivers pose a significant threat to highway safety. LPR technology has the capability to quickly identify vehicles whose registered owners have suspended or revoked licenses or registrations, making it much faster and easier for law enforcement officers to detect and apprehend suspended drivers.



Benefits to Law Enforcement: Beyond Traffic Safety

LPR's are at the forefront of discussions about the impact of technology on improving traffic and public safety. In the field of auto theft recovery and investigation, the LPR is a force multiplier for officers in the field. The technology enables reading and checking the status of thousands of license plates in a single shift, all while the investigator can watch his or her surroundings for activity, malevolent or benign. The LPR is a tireless partner, constantly on the watch

1 The National Cooperative Highway Research Program, Report 500, Volume 2.

for stolen vehicles and wanted subjects, AMBER Alerts, missing persons, and more. This technology is even more effective when there is a front and rear license plate for the LPR to read.

Many police agencies use LPR-equipped vehicles to collect plate information as they respond to bank robberies and other major crimes to capture plate numbers of vehicles leaving the area as police respond to the scene of the crime. There have been many instances when these reads have led to the identification of suspect vehicles and suspect arrests.

Public Safety Benefit

As mentioned in the previous Benefits subsections, LPR-equipped law enforcement vehicles can scan thousands of plates an hour, thus increasing the chances of finding a particular vehicle quickly, enhancing highway and public safety. One example was provided by the Utah Department of Motor Vehicles Enforcement Division, which prior to installing LPRs on their police vehicles, averaged



One example was provided by the Utah Department of Motor Vehicles Enforcement Division, which prior to installing LPRs on their police vehicles, averaged 400 stolen vehicle recoveries annually. After LPR deployment, they now scan 45,000 plates monthly and are now recovering more than 1,000 stolen vehicles annually. See Chapter 7 – License Plate Reader Success Stories for many more examples.

400 stolen vehicle recoveries annually. After LPR deployment, they now scan 45,000 plates monthly and are now recovering more than 1,000 stolen vehicles annually. See Chapter 7 – License Plate Reader Success Stories for many more examples.

It should be noted that there are circumstances when the lack of a front license plate limits the effectiveness of LPR on front-facing traffic. This is also an issue for school bus drivers who report drivers who fail to stop for the buses while loading or unloading students. These drivers often rely on the presence of a front license plate to be able to report these violations. Some tolling authorities also rely on the front plate for both revenue collection and enforcement.

Homeland Security Enhancements

LPR technology has also become an important national security tool. LPR technology is used to query the license plate numbers of vehicles entering and departing the U.S. to identify potential threats to national security. LPR units are also set up in locations in proximity to critical infrastructure to identify potential threats.

Chapter 5 License Plate Readers as a Tool to Improve Toll, Commercial Motor Vehicle, and Border Operations

Introduction

This chapter discusses how License Plate Reader (LPR) systems benefit public mobility but also have become core to the way many electronic toll systems collect tolls and enforcing payment. LPR has made it possible for the toll industry to move increasingly toward all-electronic cashless toll operations, which are permitting free-flow traffic to pay tolls at highway speeds, improving roadway efficiency, improving the customer experience, and mitigating adverse environmental impacts. Road and bridge toll collection helps provide revenue assurance for highway lane management, maintenance, and improvement.

LPR systems are also effective in commercial vehicle enforcement, which results in efficiencies in safety and traffic flow near weigh station and inspection facilities. These systems help officers identify and focus resources on the vehicles and drivers that are most likely to present safety risks.

LPR systems are also deployed by Customs and Border Protection along the U.S. borders with Canada and Mexico to improve and enhance traveler mobility across these borders.

The introduction of electronic toll collection (ETC) has reduced the dependence on toll collection personnel and manual cash transactions at toll points. Although ETC has improved traffic flow and efficiency, it has also introduced a new challenge—toll evasion and revenue loss.

Mobility and Toll Collection

Collection of user fees on roads, bridges, and tunnels—or tolls—has served as an important means of financing key transportation projects and funding ongoing operations and maintenance for as long as roads have existed. Tolls provide a direct approach to funding highways, bridges, and tunnels without increasing local or state taxes, and they ensure that those who use and benefit the most from these projects pay for them directly.

For toll facilities to be effective, however, tolls must be collected. Historically, toll collection involved staff at a gate or in a toll booth collecting cash directly from motorists and making change at strategic points along the roadway. This process required each vehicle to stop in the tolling zone for a brief period to tender a cash toll payment. When the collection site becomes a choke point – risks of rear impact and chain reaction crashes increase. Toll chokepoints also reduce the efficiency of the corridor where collection takes place. Additionally, when toll collection slows traffic, the reduced efficiency adds emissions into the environment and increases the time required to move people and commercial goods.

Over the past three decades, most toll operators modernized their toll collection systems with technology that allows for prepaid toll accounts using in-vehicle transponders to identify valid toll account holders. The introduction of electronic toll collection (ETC) has reduced the dependence on toll collection personnel and manual cash transactions at toll points. Although ETC has improved traffic flow and efficiency, it has also introduced a new challenge—toll evasion and revenue loss. Toll violators

include motorists who travel through an ETC-only lane without a transponder or unfunded toll account, creating unpaid toll transactions. This not only reduces the funding available for roadway operations and maintenance but also adversely affects fairness to those who pay their tolls, potentially eroding public support for tolling. In an ETC environment, there is a cash payment option for motorists without a transponder and prepaid toll account. LPR technology is used to capture license plate images of vehicles without toll transponders in ETC toll lanes to enforce the toll payment from the registered vehicle owner.

In recent years, toll operators are increasingly adopting all-electronic tolling (AET) operations, in which the cash payment option is eliminated entirely. Cashless AET operations offer the benefit of allowing free-flow tolling, often permitting all vehicles to move through the tolling point at the posted speed limit without stopping or slowing. AET operations are reducing the need to separate cash payment and ETC vehicles and the associated roadside infrastructure required to do so. Instead, AET operations often use overhead gantries with electronic toll equipment (e.g., antennas, transponder readers, and LPR cameras) to process the toll transaction with all vehicles.

This not only reduces the funding available for roadway operations and maintenance but also adversely affects fairness to those who pay their tolls, potentially eroding public support for tolling.

Vehicles with in-vehicle transponders pay their tolls through their toll accounts, just as they do in an ETC environment. Vehicles without toll transponders in an AET environment have their license plate images captured, and toll bills are sent to the registered owners of the vehicles to arrange payment of the toll due. In an AET tolling environment, more transactions are being processed based on LPR technology. For commercial motor vehicles, the Federal Motor Carrier Safety Administration estimates a truck will save approximately $10 per facility each time a truck is able to legally bypass a weight station or inspection facility.

Today as motor vehicle transportation solutions orient their designs toward improved mobility, reduced congestion, and more reliable levels of service, the use of LPR technologies has increased substantially. The conundrum in this development is that as LPR technologies improve, license plates continue to take on increasingly complex designs, making accurate license plate reading problematic.

According to the Federal Highway Administration (FHWA), jurisdictions throughout the U.S. are installing managed lanes (e.g., high occupancy/toll [HOT] lanes) in response to increased congestion. Managed lanes are intended to lessen congestion and provide greater mobility than the adjacent general-purpose lanes of state highways or interstate highways located in urban areas. In some cases, it is also used to enforce High Occupancy Vehicle (HOV) violations automatically, without the need of a law enforcement officer to visually detect violations. LPR also assists transportation officials to understand and influence traffic patterns and set flexible pricing based on traffic levels to reduce congestion, resulting in fewer roadway incidents and increased mobility.

Today as motor vehicle transportation solutions orient their designs toward improved mobility, reduced congestion, and more reliable levels of service, the use of LPR technologies has increased substantially. The conundrum in this development is that as LPR technologies improve, license plates continue to take on increasingly complex designs, making accurate license plate reading problematic.

Another feature of the move to LPR-related open road tolling is the use of enforcement-intended data access for revenue collection that is not law enforcement related. In jurisdictions where overhead tolling is

introduced, the department of motor vehicles should be consulted in the means by which vehicle and vehicle operator data may be obtained.

Revenue Loss

License plate designs, license plate obstruction, and purposeful avoidance to register and title vehicles are the most significant contributors to revenue losses for authorities using LPR systems. License plates that align with the AAMVA License Plate Standard will improve the effectiveness of LPRs and subsequently increase toll collections.

One toll agency with years of experience in operating a cashless AET operation that depends on license plate images to collect tolls from motorists without toll transponders indicates the following experience:

	2017		2018		2019	
Total Image Transactions	**36.930M**		**39.092M**		**41.143M**	
Reject Reason	**Total**	**%**	**Total**	**%**	**Total**	**%**
Unreadable Plate	2.058M	5.6%	2.139M	5.5%	1.901M	4.6%
Temporary Plate	1.063M	2.9%	723K	1.8%	667K	1.6%
No DMV Record	1.116M	3.0%	801K	2.0%	780K	1.9%
Other	784K	2.1%	1.061M	2.7%	978K	2.4%
Unenforceable Totals	**5.021M**	**13.6%**	**4.724M**	**12.1%**	**4.326M**	**10.5%**
Lost Revenue	**$23.1 Million**		**$25.8 Million**		**$25.3 Million**	

Although the unrecoverable revenue is significant, it should also be noted that even through a 12.1% growth in image-based transactions over three years, there was a 13.8% decline in unenforceable images. This is indicative of what the industry has experienced in terms of improvements in hardware, software, and business practices improving overall outcomes. That said, easily identifiable license plates can further mitigate lost revenue in the transportation industry as well as other businesses and enforcement models that use imagery and license plate information as the core of their revenue enforcement efforts.

Lost toll revenues amounted to $23.1 million in 2017, $25.8 million in 2018, and $25.3 million in 2019.

Mobility at U.S. Borders with Canada and Mexico

Currently, Customs and Border Protection (CBP) has three programs that use LPR to expedite entry to the U.S.—NEXUS, Secure Electronic Network for Travelers Rapid Inspection (SENTRI), and Free And Secure Trade (FAST). NEXUS is used at the Canadian border and SENTRI, is used at the Mexican border. FAST is a commercial clearance program for low-risk shipments entering the U.S. from Canada and Mexico. Each of these programs has dedicated lanes, and users are vetted.

All vehicles and persons entering the U.S. are subject to inspection. Every vehicle and every person entering at a land border port must be queried through various law enforcement databases before they can enter the U.S. Although the inspection process encompasses more than just queries, each query takes time to perform, and time is a factor in vehicle wait times. CBP, through the Western Hemisphere Travel Initiative (WHTI), has installed technology at most ports of entry that automates many functions previously done manually. This automation has resulted in reduced vehicle inspection times while maintaining the integrity of the inspection process.

Other LPR Applications That Benefit Mobility

Commercial Vehicle Enforcement

Commercial Vehicle Enforcement entities use LPR. Several specialized companies have emerged that use LPRs to read license plates and compare the plate number to federal safety data sources to ensure trucks are in compliance with federal and state motor carrier safety programs. Some systems also verify various state and federal credentials required to operate in the jurisdiction, check for out-of-service violations, and check for wants or warrants associated with vehicles.
Municipal Parking Enforcement



LPR camera in use at a roadside truck scale.

Municipal Parking Enforcement

On-street parking enforcement efficiencies have been gained by using LPR technology. With these systems, parking scofflaws who fail to pay their parking citations or fines are placed in a data source that is downloaded to an LPR-equipped vehicle. The LPR quickly identifies those who have failed to pay, which allow municipalities to boot vehicles, ensuring parking revenues are recaptured.



Mobile LPR camera mounted on parking enforcement vehicle.

In a 30-day trial conducted during 2020 using one LPR-equipped vehicle, the Long Beach Police Department in southern California identified nearly 300 scofflaws who had five or more unpaid parking citations, capturing nearly $200,000 in unpaid fines. In addition, seven arrests not associated with a parking citation were made.

Chapter 6 License Plate Reader Program Best Practices for Law Enforcement

Introduction

A properly organized and managed license plate reader (LPR) program can greatly enhance the effectiveness of patrol operations and criminal investigations. The best LPR programs are built on a foundation of good policy and training.

The measurement of success for an LPR program is subjective. Recovering stolen vehicles; arresting subjects with active warrants; and recovering AMBER, SILVER, and BLUE Alert subjects are some measures of success. However, in an era of transparency and civilian oversight, a true measure of success should include an agency's ability to collect, store, and delete millions of LPR reads in an efficient and secure manner. It should also be noted that LPR systems are only as good as the data they rely on. Ensuring that the hot lists they access are kept current is critical to limiting the possibility that users will act on erroneous information.

Policy

Law enforcement agencies can build meaningful LPR system policies that respect individuals' privacy rights while providing authorized users with the information necessary to ensure the public's safety. Policies should include LPR program goals and objectives and should not be too restrictive as to limit 'operators' ability to perform law enforcement functions yet still be protective of the massive amounts of data an LPR system collects.

Because LPR equipment and accounts can have broad permissions, policies should contain language defining what functions an operator can and cannot perform with an assigned LPR account or LPR equipment. Having operators sign an acceptable use statement is a method of tracking and ensuring each user has been made aware of the policies set forth. In addition to the policies already explained, the following specific topics and their relationship to the use of LPRs should also be reflected in policy:

- **Data retention and dissemination** – Data usage policies should conform with jurisdiction laws governing the agencies legal authority to collect, retain, disseminate, and dispose of LPR data. Agencies should have a data retention period in policy (whether it is included in jurisdiction law or not) with justification for the data retention period they choose.
- **Freedom of Information Act (FOIA)** – An agency's FOIA policy should be examined to reflect the legal standards of FOIA.
- **Data security** – Operator passwords, system lockouts, system audits, and user audits should all be addressed in policy. Many of these are already established within an agency or by an overarching governing body. Assurances should be made to maintain compliance with these existing policies.
- **Memorandums of understanding (MOU)** – Many agencies and jurisdictions may decide to work together to establish one large LPR network. This reduces the cost per agency, and the burden of responsibility is shared. An established MOU identifies the roles and responsibilities between the agencies.

See Appendix (C) for Sample LPR Policies from Ohio, Utah, and Virginia.

Training

In addition to having sound policy, formalized training should be in place that conveys the policy content to LPR system operators. Training is a fundamental component of an LPR system. Without properly documented training, operators have no direction for which to properly set up, use, and troubleshoot LPR equipment. Training should emphasize policy (and case law) surrounding data retention. This can serve to assure the public that data are being collected, stored, used, and deleted in a manner consistent with established legal guidelines and policy.



LPR training can be divided into three sections: operations, data analysis, and technical support. All sections of training should be recurring and culminate in a test. This ensures new material is presented and operators remain vigilant in the use of the LPR system.

Operations training should focus on the daily operator of an LPR-equipped vehicle. Like speed-measuring devices, the operator of an LPR-equipped vehicle should be able to set up, operate, and troubleshoot a vehicle-mounted LPR system.

Data analytics could be considered the second most important function of an LPR system.(the most important function being data collection). Having the training necessary to analyze a target vehicle across a network of LPR cameras relies on consistent and thorough training.

The last section of training which that be included in an LPR program is technical support. This section of training encompasses the logistical support staff most agencies will use to up-fit LPR patrol vehicles, monitor fixed sites, perform server maintenance, and perform system upgrades.

LPR Program Staffing

An LPR program should be adequately staffed to provide proper program support, oversight, and planning. Prior to determining staffing levels, a decision should be made if the LPR program will fall under the management and leadership of an existing police hierarchy (such as Operations or Investigations) or if it will be autonomous (specialty unit).

If an agency has fixed LPR equipment in its program, the program should be staffed sufficiently to maintain 24-hour operations to respond to any received alert, such as AMBER Alerts.

An LPR program needs enough employees to install and fix the equipment and employees who can manage both the system and equipment. If agency staffing is limited, employees can effectively multitask and meet the needs of multiple positions at once. If an agency does not have the number of employees or expertise to complete all the required aspects of running an efficient program, contractors can be employed to conduct one or more critical functions of the LPR program.

Equipment

Like staffing, LPR equipment needs to encompass all aspects of the program. A comprehensive, but non-inclusive list of equipment needed for an effective LPR program follows (mobile, fixed, and portable platforms):

MOBILE LPR	FIXED-SITE LPR	PORTABLE PLATFORM
Vehicle-mounted readers	Overhead or pole-mounted readers	Platform: commonly a trailer
Connecting wires from readers to trunk box	Continuous power supply	Continuous power supply (solar combined with battery)
Trunk box	Cellular or fiberoptic network	Cellular network
Mobile systems software	Systems software	Systems software
Mobile computer capable of operating mobile systems software		
GPS-capable antenna		



Vehicle-mounted reader.



Pole-mounted reader.



Trailer-mounted reader.



Roof-mounted LPR.



Trunk-mounted LPR.

There are many LPR manufacturers that produce reliable and durable LPR equipment. Purchasing agents need to consider the proprietary nature of LPR equipment and be aware that some products are not interoperable with others. It is critical for LPR data to properly communicate from the point of collection

(reader) to a central computer (server). LPR data must be securely protected and accessible by operators, most commonly from a desktop- or vehicle-based computer system. Legal considerations need to be addressed before purchasing equipment. For example, a cloud-based data storage system may not be compliant with a jurisdiction's data storage laws.

The specific type of LPR equipment chosen should be driven by agency mission and priorities. Whereas some agencies may prefer only mobile LPR, others may also use fixed-site LPR's, covert equipment, or portable platforms to create a robust LPR program.

When selecting LPR equipment, anticipate and plan for program expansions and logistical support needs. Items such as spare parts, storage facilities, and ancillary equipment should be considered as well.

Summary

A well-thought-out and well-executed LPR program provides law enforcement an additional tool in providing essential public safety services. Establishing an LPR program is a task that should be completed with careful consideration, planning, and organization.

Chapter 7 License Plate Reader Success Stories

Introduction

What follows are documented examples of how License Plate Reader (LPR) technology has benefited law enforcement in the performance of their public safety mission.

On **January 7, 2021**, Kristin Walker from Alabama was putting fuel into her vehicle with her two children in the backseat when a subject jumped into the driver seat to steal the vehicle. Walker was able to remove her children from the vehicle before it was highjacked. With the use of LPR technology, the Rankin County, Mississippi, Sheriff's Office was able to spot the vehicle a short time later and arrest the two subjects involved.

In **December 2020**, a North Carolina DMV License & Theft Bureau Law Enforcement Agent observed a Volkswagen traveling in a toll lane at a high rate of speed and attempted to stop the vehicle. The vehicle operator failed to stop, and with speeds near 130 mph, the pursuit was called off. LPR information was obtained from the North Carolina Turnpike Authority that included photographs of the driver, vehicle, and license plate information. The violator was located, apprehended, and charged with several serious traffic violations.

On **December 19, 2019**, A Delaware guidance counselor allegedly sexually assaulted a minor teenage boy while in Ocean City, Maryland. The victim alleged Allen Reese drove him from Delaware into Ocean City, where he sexually assaulted him. Using Ocean City's LPR, detectives were able to confirm that Reese's vehicle crossed the Route 90 bridge as well as entry and exit times consistent with the dates and times of the assault provided by the victim. Based on the evidence from the victim corroborated by the LPR system, detectives scheduled an interview with the suspect to execute a warrant and collect DNA samples. However, detectives were notified by Homeland Security that a flight to Casablanca, Morocco, had been booked for Mr. Reese. Because it appeared that he was preparing to flee the country to avoid the sexual assault charges, a warrant was immediately issued for Mr. Reese. He was quickly located and held without bond on charges of sexual abusing a minor and third-degree sexual offense.

In **August 2019**, police with Duck, North Carolina, Police Department (an Outer Banks Island community) deployed their LPR systems to find residents who stayed on the island during a mandatory evacuation during Hurricane Dorian. LPR cameras recorded the plate numbers of vehicles exiting the island to determine which registered vehicles did not leave. The homes associated with those vehicles were visited by police to warn those residents of the risks of remaining on the island.

On **July 24, 2019**, a woman put her dog Happy into her car in Baltimore's Guilford neighborhood. She was just getting into the driver's seat when she was forcibly pulled her from her car and several suspects got into her car and sped off. Happy was still in the car when the suspects fled. The woman notified police, and the Baltimore Police Department immediately placed the license plate on an LPR hotlist as a carjacked vehicle. Soon after a patrol officer passed by the vehicle, which

was parked and unoccupied, and received an alarm on the LPR system he was operating. He approached the car and saw that Happy was still inside with the windows closed and doors locked. Because it was a hot July day, the officer smashed a window and rescued Happy before he was overcome from the heat. The woman and Happy were soon reunited.

On **July 15, 2020**, a man shot and killed his ex-girlfriend in the parking lot of her workplace in Springfield, Tennessee. Two days later, the suspect drove through Mt. Juliet, where a Mt. Juliet Police Department (MJPD) vehicle equipped with an LPR system detected the suspect vehicle license plate, alerting the officers who arrested the suspect.

According to MJPD Chief James Hambrick, "It's amazing the stuff that you wouldn't know travels through your city … is actually traveling through your city." That's one of many success stories to come out of the MJPD's use of LPR, Chief Hambrick said.

On **June 30, 2018**, a subject in Sacramento, California, was attempting to cross a street in his wheelchair and was hit and killed by a passing motorist who failed to stop and render aid. The license plate belonging to the vehicle that left the scene was detected by LPR, and the driver was arrested for felony hit and run.

On **March 15, 2018**, James Allen Hayes plead guilty in federal court to committing multiple bank robberies over the course of five months throughout California. Hayes was apprehended as a result of LPR detecting his vehicle traveling between robbery locations.

Robert Sheets was accused of shooting a man on **August 13, 2017**, in Manor Township, Pennsylvania. Sheets returned to the suspect the next day and discovered him still alive. He then shot the victim again, leaving him for dead and fleeing the area. Miraculously, the victim survived and was able to identify the man who tried to kill him as Sheets. The vehicle driven by Sheets was immediately filed in National Crime Information Center as a felony vehicle, which resulted in a hotlist entry on LPR systems across the U.S.

A few days later, in Fairfax County, Virginia, an LPR alerted officers that Sheets was connected to a 2007 Ford Edge heading west on I-66. Fairfax police cruisers pulled in behind Sheets, and after a 38-mile pursuit, Sheets was apprehended.

On **August 26, 2015**, a gunman shot and killed a news anchor and cameraman from a local news station (Alison Parker and Adam Ward) while they were doing a report in Roanoke, Virginia. The license plate number of the shooter was broadcast statewide. Several Virginia State Police patrol vehicles were equipped with LPR. Five hours later and approximately 200 miles away from the shooting scene, Virginia State Police Trooper Pam Neff entered the license plate number into her LPR and discovered the LPR had just read the suspect license plate three minutes prior. Trooper Neff was able to catch up to the suspect vehicle and when back-up was in position proceeded with the apprehension. Trooper Neff was recognized by AAMVA during the AAMVA Annual International Conference in Williamsburg, Virginia, in August 2016.

For more news stories about law enforcement LPR successes from September 2017 to September, 2018, go to https://www.theiacp.org/sites/default/files/ALPR%20Success%20News%20Stories%202018.pdf

Appendix A Significant License Plate Reader Court Cases and Applicable Federal Statutes

United States Court of Appeals for the Ninth Circuit
United States v. Jay Yang,
958 F.3d 851 (9th Cir. 2020).
May 4, 2020
https://law.justia.com/cases/federal/appellate-courts/ca9/18-10341/18-10341-2020-05-04.html

Jay Yang was observed stealing mail from U.S. mail collection boxes on surveillance cameras driving a rented GMC vehicle beyond the rental contract due date. The license plate number was observed and searched in a License Plate Reader (LPR) database, which helped lead investigators to his home. Yang claimed because his rental agreement was past due and the contract was no longer valid when the plate was observed by LPR, the LPR data were invalid, and anything obtained from the search of his residence was not admissible. The court ruled there is no expectation of privacy of a license plate regardless if rental contract was expired. The LPR database did not reveal all the defendant's movements and therefore did not infringe on reasonable expectation of privacy.

United States Court of Appeals for the Eleventh Circuit
United States v. Larry Lamar Wilcox,
415 F. App'x 990 (11th Cir. 2011).
February 28, 2011
https://law.justia.com/cases/federal/appellate-courts/ca11/10-13031/201013031-2011-02-28.html

Larry Wilcox argued the use of LPR technology amounted to unconstitutional surveillance violating his reasonable expectation of privacy. The defendant said the district court erred in denying a motion to suppress, stating an Atlanta police officer's use of LPR technology violated his Fourth Amendment right to be free from an unreasonable search.

The Court of Appeals ruled that the Supreme Court had concluded in similar contexts visual surveillance of vehicles in plain view does not constitute an unreasonable search for Fourth Amendment purposes. Given the Supreme Court's Fourth Amendment precedent, the Court of Appeals ruled the district court did not commit plain error in concluding Wilcox did not have a reasonable expectation of privacy in the plainly visible license plate and the officers' use of LPR did not violate the Fourth Amendment.

United States Supreme Court
United States v. Knotts,
460 U.S. 276, 103 S.Ct. 1081, 75 L.Ed.2d 55 (U.S. 1983).
December 1983
https://supreme.justia.com/cases/federal/us/460/276/

Tristian Armstrong was being investigated for stealing chemicals to manufacture illegal drugs. Agents attached a radio transmitter to a container of chemical sold to Armstrong, which tracked the location of where methamphetamine was being produced by Leroy Knotts. A search warrant was obtained, and an illegal drug manufacturing lab was discovered.

Knotts was convicted in district court, but the U.S. Court of Appeals reversed the conviction, stating Knotts' Fourth Amendment rights were violated by use of the tracking device, and the evidence could be suppressed. The U.S. Supreme Court held the initial conviction, ruling the tracking device did not invade any legitimate expectation of privacy and was neither a "search" nor a

"seizure" by grounds of the Fourth Amendment. The movement of a person traveling on a public highway does not afford an expectation of privacy of the movements. Nothing indicated the tracking device was used to gather information from within the private area.

Privacy and Fourth Amendment

Authority for Police to Check License Plates
United States Court of Appeals for Ninth Circuit
***United States v. Ismael Diaz-Castaneda*,**
494 F.3d 1146 (9th Cir. 2007).
July 18, 2007
https://caselaw.findlaw.com/us-9th-circuit/1468527.html

An officer ran the license plate on a pickup traveling in front of him in traffic. The plate information response indicated that the driver's license of the registered vehicle owner, Solia Diaz, was suspended. The officer, believing the operator fit the description of Diaz, stopped the vehicle. Diaz was arrested for driving while under suspension. The vehicle passenger, Ismael Diaz-Castaneda, was found to have an immigration detainer on him and was arrested.

Diaz-Castaneda argued the stop violated his Fourth Amendment rights, and any subsequent evidence should be withheld. The court held a license plate check does not constitute a Fourth Amendment search, and evidence should not be suppressed.

U.S. Court of Appeals for Sixth Circuit
United States v. Curtis Ellison,
462 F. 557 (6th Cir. 2006).
September 5, 2006
https://caselaw.findlaw.com/us-6th-circuit/1031532.html

A Farmington Hills, Michigan, police officer ran a license plate of a parked vehicle through a police telecommunication system belonging on a vehicle operated by Curtis Ellison. Information returned revealed the registered owner was a "wanted person." Ellison was determined to be a passenger in the vehicle and was arrested. District court originally ruled the officer did not have probable cause to run the plate because the van was not parked illegally, and therefore Ellison Fourth Amendment Rights were violated. The court determined what a person exposes publicly is not subject to Fourth Amendment protection, and observing a license plate displayed in plain view does not constitute a search.

Validity of License Plate Reader Technology

United States Court of Appeals for the Third District
***United States v. Marcus White*,**
504 F. App'x 168 (3d Cir. 2012).
November 15, 2012
https://law.justia.com/cases/federal/appellate-courts/ca3/11-4035/11-4035-2015-04-29.html

Marcus White was convicted in Pennsylvania for his involvement in robberies of a post office and convenience stores. White's vehicle had been reported stolen and was detected by a Maryland state police trooper by an alert from an LPR while on patrol. During the suppression hearing, the District Court noted "the technology used by the license [plate] reader is verifiable and acceptable technology." White did not challenge this conclusion.

Use of License Plate Reader Data

Supreme Court of Virginia
Opinion of Justice Stephen R. McCullough
Harrison Neal v. Fairfax County Police Department, ET AL,
299 Va. 253, 849 S.E.2d 123 (Va. 2020).
October 22, 2020
https://law.justia.com/cases/virginia/supreme-court/2020/191127.html

In a prior ruling, the Virginia Court of Appeals ruled the "passive use" of LPR data by Fairfax County, Virginia, police violated the Virginia Data Act. Neal

argued the police department could not collect and store passively obtained LPR data without suspicion of criminal activity. Neal claimed the Virginia Data Act prohibited the gathering of personal information unless justified by law. The court initially ruled the LPR data provided a link to identify the vehicle owner and therefore LPR data was subject to the Virginia Data Act.

In a later ruling from the Virginia Supreme Court, the court stated the LPR system did not qualify as an information system because it did not contain name, personal number, or other identifying particulars of data for a subject. The court further stated the plate, vehicle photo, date, time, and GPS location did not bring the Data Act into play because the LPR system did not contain all the components and operations of a record keeping process. The court found the police department's passive use of the LPR system was legal.

Massachusetts Supreme Court
***Commonwealth of Massachusetts v. McCarthy*,**
484 Mass. 493, 142 N.E.3d 1090 (Mass. April 16, 2020).
https://law.justia.com/cases/massachusetts/supreme-court/2020/sjc-12750.html

Law enforcement officers were investigating Jason McCarthy's suspected illegal drug activity and deployed LPRs on bridges to track his activity. Police used data from the LPRs and received real-time alerts, which led to the arrest of McCarthy. McCarthy filed motion to suppress the LPR data because it violated his constitutional right to privacy of his public movements. The court ruled the defendant's privacy was not violated because of the limited extent and use of the LPR data.

Reasonable Suspicion for Vehicle Stop Based on License Plate Reader Information

United States Court of Appeals for the Ninth Circuit
Denise Green v. City and County of San Francisco,
751 F.3d 1039 (9th Cir. 2014).
May 12, 2014
https://caselaw.findlaw.com/us-9th-circuit/1666208.html

An LPR operated by a San Francisco Police officer indicated a license plate displayed on Denise Green's vehicle was on a stolen vehicle. A high-risk felony stop occurred, and Green was held at gunpoint, handcuffed, and detained. Eventually, officers ran the actual plate to confirm stolen and determined the LPR misread the plate, and the vehicle was not stolen; Green was released.

San Francisco Police Department officers are trained that an LPR hit does not automatically justify a vehicle stop. Officers are directed to verify validity of the identified hit before executing a stop. Officers are instructed to verify the plate being read by the LPR is truly the plate on the vehicle and to confirm the stol-en "hit" with their police telecommunications system. **The court ruled an unconfirmed LPR "hit" does not form a reasonable suspicion to support an investigatory detention of subject.**

Georgia Court of Appeals
Hernandez-Lopez v. The State of Georgia,
319 Ga. App. 662, 738 S.E.2d 116 (Ga. Ct. App. 2013).
February 5, 2013
https://caselaw.findlaw.com/ga-court-of-appeals/1622591.html

An LPR in use by an officer with the Gwinnett County, Georgia, Police Department indicated a plate belonged to a "wanted person" by the name of Eloy

Hernandez-Lopez. The officer noted a warrant was for an adult male, which matched the warrant identifying information. The vehicle was stopped and the subject operating the vehicle was determined to be Salomon Hernandez-Lopez, and he was arrested for operating without a license.

Hernandez-Lopez claimed the officer lacked reasonable suspicion to conduct a traffic stop based on the LPR information. The court held the officer did in fact have reasonable suspicion based on the LPR information indicating the license plate belonged to a "wanted person." This would be the same as if an officer ran the license plate through the Georgia police telecommunications system directly. **The court ruled an LPR "hit" provides an officer with reasonable suspicion to justify an investigatory stop.**

New York Supreme Court
***People of the State of New York v. Luis Davila, Jr.*, 27 Misc.3d 921, 901 N.Y.S.2d 787 (N.Y. Sup. Ct. 2010), *aff'd*, 137 A.D.3d 655, 26 N.Y.S.3d 862 (N.Y. App. Div. 2016).**
April 1, 2010
https://law.justia.com/cases/new-york/other-courts/2010/2010-20111.html

A New York Police Department LPR mounted on a police vehicle alerted officers to a suspended plate, and the vehicle was stopped. An officer observed what appeared to be a weapon in possession of a vehicle occupant and subsequently arrested the subject for possession of a firearm. Davila contested the arrest, arguing the officer failed to follow department policy by first verifying the LPR data had been updated in the past 24 hours and did not verify the information against the department database. The court ruled the department policies are guidelines and not required by law; therefore, use of LPR to detect the vehicles registration as suspended was lawful.

Related Federal Statutes

28CFR Part 23 Criminal Intelligence Systems Operating Policies
28 CFR Part 23 contains policy standards for law enforcement agencies operating federally funded multijurisdictional criminal intelligence systems. The standards specifically provide guidance for the submission, entry, security, inquiry, dissemination, review, and purge of criminal intelligence information.

2 CFR § 200.79 Personally Identifiable Information (PII).
LPR information is NOT PII
PII is information considered capable of identifying an individual either by itself or with other identifying information. LPR systems contain information consisting of vehicle license plates, vehicle photos, dates, times, and GPS locations—information generally not considered PII. Therefore, LPR information may not be restricted by statutes concerning maintaining PII but can become PII if additional information is included that is defined as PII. Case-by-case assessment is recommended when developing LPR system data maintenance and use.

Driver's Privacy Protection Act (DPPA) of 1994, 18 U.S.C. 2721
The Driver's Privacy Protection Act (DPPA), 18 U.S.C.A. §§ 2721-25 also supports the premise that a license plate number alone is not PII. Enacted in 1994, the DPPA is a federal law that regulates how state motor vehicle departments release information contained in their records. DPPA addresses the prohibition on release and use of certain personal information from state motor vehicle records. Collected LPR information contains no PII that may be used to connect a license plate detection to an individual. It is only with permissible purpose law enforcement may make this connection (using motor vehicle records).

Appendix B Additional License Plate Reader Resources

American Association of Motor Vehicles (AAMVA)

AAMVA – Best Practices and Model Legislation

- License Plate Standard, Edition 2 (2020)

AAMVA – AAMVA Policy Positions

- Alternative License Plates Policy Statement (Adopted 2020)
- License Plates Policy Statement (Amended 2020)
- License Plates Should Not Be Obscured Policy Statement (Amended 2020)
- Temporary License Plates Policy Statement (Amended 2020)

International Association of Chiefs of Police (IACP)

You must be an IACP member with log-in credentials to access these resources:

https://www.theiacp.org/resources/policy-center-resource/license-plate-readers

- IACP License Plate Reader Model Policy (2010)
- IACP License Plate Reader Concepts and Issues Paper (2010)

These IACP resources are publicly accessible:

https://www.theiacp.org/projects/automated-license-plate-recognition

- IACP License Plate Reader Privacy Impact Assessment (2009)
- IACP License Plate Reader Policy & Operational Guidance (2012)
- IACP Resolution: Retro-Reflective Front and Rear Plates (2018)
- IACP Resolution: Digital License Plates (2020)
- IACP Technology Policy Framework (2014)

Police Executive Research Forum

Free Online Documents (policeforum.org)

- Combating Auto Theft in Arizona: A Randomized Experiment with License Plate Recognition Technology: Police Executive Research Forum, December 2011

RAND Corporation

https://www.rand.org/pubs/research_reports/RR467.html

- License Plate Readers for Law Enforcement – Opportunities and Obstacles (2014)

Appendix C Sample License Plate Reader Policies

Introduction

The core business values that License Plate Reader (LPR) promises can only be achieved through proper planning, implementation, training, deployment, use, and management of the technology and the information it provides. Like all tools and technologies available to law enforcement, LPR must also be carefully managed. Agencies must clearly articulate their strategic goals and tactical objectives for the technology, and this strategy should be tightly aligned with the broader strategic plans of the agency. Thorough and ongoing training is required to ensure that the technology performs effectively and that users are well versed in the operational policies and procedures defined and enforced by the agency.

Policies must be developed and strictly enforced to ensure the quality of the data, the security of the system, compliance with applicable laws and regulations, and the privacy of information gathered. Building robust auditing requirements into agency policies will help enforce proper use of the system and reassure the public that their privacy interests are recognized and respected.[1]

Three agency sample policies follow:

Ohio State Highway Patrol

Utah Tax Commission, Motor Vehicle Enforcement Division

Virginia State Police

1 IACP ALPR Policy & Operational Guidance (see Appendix B).

OHIO STATE HIGHWAY PATROL POLICY

Summary of Revisions

Revisions are in red, bold, italics throughout.

Purpose

To provide guidelines for the implementation, installation, and use of mobile and stationary Automatic Plate Reader (APR) technology and equipment at selected locations to scan, detect, and identify license plate numbers appears on selected "Hot Lists."

Policy

A. **STATEMENT OF POLICY –** The Ohio State Highway Patrol will utilize APR technology in patrol cars and at stationary locations to accurately identify license plates ***linked to criminal activity and/or commercial motor vehicle administrative violations.***

B. **FUNCTIONALITY AND OPERATION <41.3.9a>**

1. **Installation –** Stationary and mobile scanners will be installed at selected locations and on selected marked and unmarked vehicles. ***GHQ electronic technicians are responsible for maintaining a list of all locations and vehicles equipped with APR technology.***

2. Data Sources for "hits" – All APRs have the ability to match a captured image to two categories of databases: criminal violations and commercial motor vehicle violations. Officers and MCEIs have the ability to match images with one or both types of databases simultaneously.

a. Criminal Databases: Both mobile and stationary APRs can match captured images with LEADS and NCIC entries with an associated license plate (e.g., stolen motor vehicles, felony warrants, missing persons, protection orders, etc.)

b. Commercial Motor Vehicles – Both mobile and stationary APRs can match captured images with the Federal Motor Carrier Safety Administration PRISM database for commercial motor vehicles placed out of service and ones with an "Inspect" or "Possible" score in the Inspection Selection System (ISS).

3. General Operation – The Division's automatic plate readers capture images of numbers and letters resembling license plates and match those captured images to the current "hot list." The "hot list" is the master index of license plates entered in both data sources listed above. The criminal database "hot list" is updated twice daily and the commercial motor vehicle database "hot list" is updated once daily.

4. Units assigned to enforcement vehicles equipped with mobile APR systems shall ***verify the receipt of*** the most recent "Hot List" from the applicable databases at the beginning of each shift.

5. **Probable Cause** – An APR "hit" from the criminal databases shall not be used as probable cause for a traffic stop or enforcement contact. Contact with the vehicle and occupants shall only be made after the "hit" is confirmed through LEADS/NCIC.

6. **Manual Entry by User into "Hot List" Database** – ***The system does not obtain real***

time information from LEADS/NCIC; therefore, there may be situations which require an officer or dispatcher to manually enter a vehicle registration into the database. These situations include, but are not limited to: active Amber Alerts, Ohio Blue Alerts, endangered missing child alerts, endangered missing adult alerts, BOLOs, and other emergency messages/alerts. Manual entry of a plate into the "Hot List" shall only be done with supervisor approval. See User Manual for entry procedures.

A "hit" on a BOLO that is manually-entered into the system shall not be used as probable cause for a traffic stop or enforcement contact.

7. **'O' vs. Zero** – Because of standardized NCIC formats, a letter 'O' and a zero in a license plate number are synonymous in NCIC records. Therefore, the "hot list," NCIC, and the APR read the letter 'O' as a zero. Any plate entry, including any manually entered by an officer or a dispatcher with an 'O' is automatically converted to a zero.

8. **Fixed Point and APR Notification** – When a license plate entered in the "Hot List" is detected by a stationary APR, a notification is automatically sent by the APR system to an OSP dispatch facility equipped to receive the notifications. When a mobile APR detects a "Hot List" entry, the officer receives an audible and visual notification on the in-car MCT.

9. **Case Documentation** – A record of the APR "hit" shall be included in the case/incident report. All "hits" captured by the APR system shall be stored for 30 days and will then be automatically purged. All "hits" will be stored electronically in the ELSAG system. Access to the ELSAG system is limited to authorized personnel only. <41.3.9b,d>

10. **Storage of "Non-Hits"** – All "non-hit" APR captures shall be automatically purged from the system within a 24-hour period. APR captures shall not be collected, stored, or shared with the intent of data mining. Dispatchers assigned to Cleveland and the Statehouse shall query the system for plates older than 24-hours on a quarterly basis to ensure "non-hit" captures are being deleted in accordance with this policy. Troopers assigned APR equipped enforcement vehicles shall perform the same query as part of the semi-annual vehicle inspection. <41.3.9d>

11. **Training –** Dispatchers, sworn officers, electronic technicians, motor carrier enforcement inspectors, and network administrators shall receive appropriate training from qualified OSP staff or vendor representatives prior to using or maintaining the APR equipment. <41.3.9c>

C. **USER MANUALS –** The manufacturer's user manuals, which provide operational procedures for both the Mobile Auto-Detector User and Operations Center Personnel are attached to this policy.

D. **GUIDELINES FOR USE <41.3.9a>**

1. **Stationary APRs**

   a. **Notification** – After receiving a "hit" through LEADS/NCIC, the dispatcher will verify the APR "hit" on the plate matches the image and follow established procedures to check NCIC/LEADS. The dispatcher will then dispatch an officer to intercept the vehicle. Two officers will be dispatched to verify "hits" at the Statehouse Garage. The officer(s) will be notified of the reason for the "hit," that the dispatch is a result of the APR and that the "hit" has been verified through NCIC.

   b. **Verification of Hit** – If, for any reason, the APR "hit" cannot be verified through LEADS/NCIC, the vehicle is not to be stopped based solely on the APR. If the

Ohio State Highway Patrol Policy (continued)

dispatcher cannot read the digital image sufficiently to verify the license plate number and state, an officer may be dispatched to intercept the vehicle, however the intercepting officer must first verify the "hit" through NCIC prior to stopping the vehicle.

c. **Turnpike Gate Personnel** – If an officer is unavailable to immediately intercept a valid "hit," the dispatcher may notify additional personnel to be on the lookout for the suspect vehicle. Ability to identify the vehicle, reason for the "hit," and known direction of travel should all be used to determine whether additional personnel should be notified. If the vehicle is observed, they should be instructed to notify the dispatch facility of the route and direction of travel.

d. Officers and dispatchers should use their discretion based on hazards, proximity of assisting officers, type of "hit," etc.

e. **Cleveland Dispatch Center / Capitol Square Parking Facility**

i. The APR system will be checked by the dispatcher at the beginning of the shift and the information will be logged on the OTIS HP-53 using File 1 – Sub Category "APR."

ii. The Statistical Analysis function will determine if the APR is functioning correctly. The system should indicate a number of plates that have been checked. If there are no plates indicated, the system is not functioning. If the system shows that plates are being scanned, the system is working correctly.

iii. The Statistical Analysis section is found in section 6 of the User's Guide.

2. ***Mobile APRs***

a. Mobile APRs are operational as long as the officer is logged in to the MCT in the vehicle.

b. Officers have the ability to toggle between the Criminal and Commercial databases or they can activate both. If both databases are active, the mobile APR will indicate a "hit" on a violation in either system.

c. Officers must verify the "hit" through LEADS/NCIC prior to stopping the vehicle. If, for any reason, the APR "hit" cannot be verified, the vehicle is not to be stopped based solely on the APR. Officers only need to verify that the plate matches the "hit" in the FMCSA database.

d. Officers and MCEIs should use their discretion based on hazards, proximity of assisting officers, type of "hit," etc.

e. Motor Carrier Enforcement Inspectors may not stop a commercial motor vehicle for the sole purpose of a LEADS/NCIC "hit".

3. **Infrastructure Specialist and Electronic Technicians are responsible for:** <41.3.9b>

a. Equipment and software deployment and installation

b. Coordinating maintenance and repair

c. Coordinating the establishment of parameters for download of NCIC and LEADS

Ohio State Highway Patrol Policy (continued)

data, pick-up radius restrictions, misdemeanor and/or felony warrants.

d. Ensure all captures on stationary and mobile APRs follow the appropriate retention schedule.

4. **Public Affairs -** All media contacts will be coordinated through the Public Affairs Unit, which shall be consulted prior to releasing any information to the news media.

5. **Licensing and Commercial Standards**

   a. LCS units may stop commercial motor vehicles for the purpose of inspection based on hits received from the PRISM file "Hot List."

   b. The reason code LPRI (License Plate Reader Inspection) will be used in ASPEN for all inspections conducted based on a PRISM hit.

Policy
410

Utah Motor Vehicle Enforcement Division
Po icy Manua

Automated License Plate Readers (ALPRs)

410.1 PURPOSE AND SCOPE

ALPR is a computer-based system that utilizes special cameras to capture a color image, as well as an infrared image, of the license plate of a passing vehicle. The infrared image is converted into a text file utilizing Optical Character Recognition (OCR) technology. The text file is automatically compared against an “informational data file” containing information on stolen or wanted vehicles as well as vehicles associated with AMBER alerts, warrant subjects or other criteria. If a match is found, the user is notified of the vehicle “hit” by an audible alert and an associated notation on the user’s computer screen.

ALPR cameras can be mobile (mounted on vehicles) or on fixed positions such as freeway overpasses or traffic signals. ALPR systems mounted on vehicles have all the necessary equipment to scan plates, notify the user of a vehicle hit, and store the plate scan data for uploading into the ALPR server at a later time. ALPR fixed positions transmit plate scan data to the ALPR server as they are scanned and notify a central dispatch, such as a station desk, of any vehicle hit.

ALPR cameras can photograph thousands of plates in a shift. All plate scan data collected from the ALPR cameras are transmitted to an ALPR server. The ALPR server resides within the State of Utah Data Network Center. In addition to software applications that are used to run the ALPR server, the ALPR server also houses the “informational data file” containing wanted, stolen, or vehicles of interest, as well as all the plate scans captured by the ALPR cameras.

The informational data file is comprised of information from the Stolen Vehicle File (SVF), “HOT FILE” (HF), Wanted Persons File (WPF), Stolen Plate File (SPF), Revoked Registration File (RRF), Cancelled Registration File (CRF), Expired Registration File (ERF), Out of Service (OS), and user defined “hot lists.“ The Informational data file is updated throughout the day with different data sources being “refreshed” at different intervals. SVF/WPF/SPF/RRF/ERF/OS data is refreshed from the state database daily, HF data is refreshed from the Bureau of Criminal Investigation hourly, CRF data is refreshed weekly, and hot list data is refreshed upon input into the ALPR server. It is important that ALPR users take into account the amount of lag time between receiving an ALPR hit notification and the last updating of the informational data file within the mobile ALPR unit database. When possible, confirm that the mobile ALPR unit hit information is still valid, either through your Communication Center (CC) or via your laptop computer (LC) prior to taking police action. Confirmation can be deferred in rare circumstances (i.e. special investigative units) when compelling circumstances may exist that, if CC is contacted, it could jeopardize the investigation and/or officer safety.

Fixed ALPR cameras have a continuous connection to the ALPR server. They are capable of uploading plate scan data to the ALPR server as the scans occur. ALPR scans can be compared against the informational data file immediately when the data sources are updated. Mobile ALPR units do not have a continuous connection to the ALPR server. In order to facilitate the exchange of data, air cards are used which will allow connectivity to the ALPR server via wireless transmission.

Copyright Lexipol, LLC 2020/08/26, All Rights Reserved.
Published with permission by Utah Motor Vehicle Enforcement Division

Utah Motor Vehicle Enforcement Division

Po icy Manua

Automated License Plate Readers (ALPRs)

If the air card in the vehicle is connected to a service, the ALPR will continually “sync” which will upload plate scan information from the vehicle to the ALPR server and/or download the latest informational data file from the ALPR server to the vehicle. It is imperative that mobile ALPR users sync their mobile units at least once at the beginning of their shift to ensure they have the latest informational data available.

410.2 POLICY AND PROCEDURES

Mobile ALPR unit users receiving an alert shall confirm the status of the vehicle by running the license plate either manually via the LC or over the radio via CC, unless compelling circumstances are present or officer safety issues make it unsafe to do so.In such cases, Officers shall confirm the status of the alert as soon as possible. When requesting CC to confirm the status of an ALPR alert, the officer shall advise CC the request is for an ALPR alert.

In the case of a stolen vehicle alert, personnel may regard the vehicle as a known stolen vehicle, while awaiting a secondary confirmation. If the decision is made to initiate a “felony stop” due to an ALPR alert on a stolen vehicle, officers shall advise CC they are following a vehicle due to an ALPR stolen vehicle alert prior to receiving a secondary confirmation by LC/CC.

Officers shall adhere to the Department’s pursuit policy as described in the Manual of Policy and Procedures. CC shall immediately provide secondary confirmation or advise the unit that the vehicle is not reported as stolen.

When Desk Personnel receive an alert from a fixed ALPR system, which is the result of an image taken from a fixed camera, they shall confirm the current status of the vehicle via their CAD terminal or via CC. While waiting for confirmation, desk personnel will advise field patrol units of the ALPR alert, the location, the vehicle description, request aero bureau, and coordinate responding field units.

410.2.1 HOT LISTS

Hot lists are comprised of user defined data that is manually input into the informational data file so that ALPR users will be alerted whenever a “vehicle of interest” is located.Hot lists can be loaded into a specific station area vehicle or to ALPR all vehicles countywide.

Hot lists can be input into the ALPR server informational data file only by ALPR administrators. Unit commanders, or their designees, must approve hot list information that is intended for use solely in their area cars. With the exception of AMBER alert information, hot list information intended for Department-wide use must have the approval of the Division Director, or his designee.Mobile ALPR users can input individual license plates into their patrol vehicle’s ALPR system for use during their shift, however, the information will be deleted from that mobile ALPR unit once user performs an “end shift” and the vehicle syncs with the ALPR server. An ALPR vehicle alert identified via hot list information does not automatically provide ALPR users with sufficient justification to pullover or detain vehicle occupants. Often times, these hotlists will identify a “vehicle of interest” which is not necessarily wanted for a crime (ex: sex offender vehicle).

Copyright Lexipol, LLC 2020/08/26, All Rights Reserved.
Published with permission by Utah Motor Vehicle Enforcement Division

Utah MVED Policy (continued)

Personnel must use discretion and in some cases have independent information justifying a traffic stop.

410.3 ALPR OPERATION

Use of an ALPR is restricted to the purposes outlined below. Department personnel shall not use or allow others to use, the equipment or database records for any unauthorized purpose.

(a) An ALPR shall only be used for official and legitimate law enforcement business (Utah Code 41-6a-2003).

(b) An ALPR may be used in conjunction with any routine patrol operation or official investigation. Reasonable suspicion or probable cause is not required before using an ALPR.

(c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

(d) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

(e) If practicable, the investigator should verify an ALPR response through the Utah Department of Public Safety (DPS) law enforcement information system or other appropriate database before taking enforcement action that is based solely upon an ALPR alert.

(f) No ALPR operator may access the DPS database or other system unless otherwise authorized to do so.

410.4 ALPR DATA COLLECTION AND RETENTION

All data and images gathered by an ALPR are for the official use of the Utah Motor Vehicle Enforcement Division and because such data may contain confidential information, it is not open to public review. ALPR information gathered and retained by this department may be used and shared with prosecutors or others only as permitted by law (Utah Code 41-6a-2004).

The Administration Lieutenant is responsible to ensure proper collection and retention of ALPR data, and for transferring ALPR data stored in department vehicles to the department server on a regular basis, not to exceed 30 days between transfers.

All ALPR data downloaded to the server should be stored for the minimum period established by department records retention guidelines and thereafter should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action. In no event shall data be maintained longer than nine months unless it is subject to a warrant, preservation request or disclosure order (Utah Code 41-6a-2004). Data that will not be purged should be downloaded from the server onto portable media and booked into evidence.

Copyright Lexipol, LLC 2020/08/26, All Rights Reserved.
Published with permission by Utah Motor Vehicle Enforcement Division

410.4.1 NON-GOVERNMENTAL AGENCY ALPR
ALPR data captured by a non-governmental agency device may only be obtained pursuant to a warrant or a court order (Utah Code 41-6a-2005).

410.5 ACCOUNTABILITY AND SAFEGUARDS
All saved data will be closely safeguarded and protected by both procedural and technological means. The Utah Motor Vehicle Enforcement Division will observe the following safeguards regarding access to and use of stored data:

(a) All non-law enforcement requests for access to stored ALPR data shall be referred to the Office Manager and processed in accordance with applicable law.

(b) All ALPR data downloaded to the mobile workstation and server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

(c) Persons approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

(d) Such ALPR data may be released to other authorized and verified law enforcement officials and agencies at any time for legitimate law enforcement purposes.

(e) ALPR system audits should be conducted on a regular basis.

Copyright Lexipol, LLC 2020/08/26, All Rights Reserved.
Published with permission by Utah Motor Vehicle Enforcement Division

Virginia State Police Policy

Virginia Department of State Police

General Order OPR 1.20 **License Plate Reader Operating Procedures**

Purpose: To establish uniform guidelines for License Plate Reader operations by Department personnel.

1. The License Plate Reader (LPR) program is intended to enhance law enforcement operations related to homeland security and terrorist watch lists, stolen vehicles and license plates, sex offender violators, wanted and missing persons, and other vehicle-related crimes that impact the safety of citizens.

2. The Director of the Bureau of Field Operations (BFO) shall appoint a Statewide LPR Program Coordinator who shall be responsible for the daily operations of the LPR Program.

Guidelines for Use

3. The Department's LPR system shall be used for official law enforcement purposes only. No employee may use, or authorize the use of, the equipment or database records for any other reason. Misuse of equipment or database records may result in disciplinary action.

4. LPR units will be installed in Department vehicles as determined by the Director of BFO or his/her designee. The Director of BFO must pre-approve the transfer of an LPR unit to another Area. Otherwise, if a sworn employee assigned a vehicle equipped with an LPR unit is transferred, promoted or resigns, the vehicle will be reassigned to another sworn employee and retained in the original Area.

5. LPR-equipped vehicles may be used for routine patrol or during special events. In all instances, LPR-equipped vehicles shall be operated in accordance with Department policies regarding vehicle operations.

6. Each employee assigned an LPR unit is responsible for ensuring they are operating with the most current "Hotlist" at the beginning of each shift. The Statewide LPR Program Coordinator should be contacted immediately if problems are encountered with the updating of the LPR units.

7. Upon receiving an alarm or hit, the sworn employee shall verify the accuracy of the information by contacting the Communications Center per established Department policy.

Effective Date – 10/1/2018 Review Date – 7/1/2022
BFO

General Order OPR 1.20

a. An LPR alarm alone is NOT sufficient probable cause to warrant a stop or arrest.

b. Sworn employees are required to confirm a positive hit prior to any enforcement action being taken.

8. Sworn employees are required to ensure that all positive hits on the Terrorist Watch List are reported to the Terrorist Screening Center (TSC) and Virginia Fusion Center (VFC) immediately. All Terrorist Watch List hits will be handled by MDT or telephone. There will be no radio traffic concerning terrorist hits except in the case of emergencies.

9. Special circumstances, such as AMBER Alerts or critical incidents, may require immediate manual updating of the LPR system "hot list." Sworn employees in possession of license plate information related to such circumstances will immediately enter the data into the LPR system. The Virginia Fusion Center (between 0600 and 2200 hours) and/or Statewide LPR Program Coordinator will ensure that new information is uploaded or relayed to all active LPR units. If a critical situation requires manual entry of license plate data, the Communications Center shall immediately notify all LPR users of the new data in the Division and document this action in the CAD system. LPR users shall manually enter the license plate information associated with the critical incident. The Communications Center shall also contact the Virginia Fusion Center and provide the information so that the data may be entered into the statewide list.

10. Terrorist organizations have openly voiced their desire to attack venues where large crowds gather, such as major sporting events, large festivals, etc. Because of the potential of just such an incident, stationary, mobile, and covert LPR use is permitted for such events. Prior to utilizing LPRs at these venues, the affected Division Commander shall submit a letter, through channels, to the Superintendent describing the event, potential threat, and parameters under which the LPRs will be utilized. The decision to grant the approval rests with the Superintendent's Office.

11. Fixed and/or covert LPR units may be used to support on-going criminal investigations or approved venues. The use of fixed and/or covert LPR units shall be coordinated with the Statewide LPR Program Coordinator.

12. At the end of each month, Monthly Plate Reader Activity Logs will be submitted to the appropriate Area Office and Division LPR Coordinator by personnel using an LPR unit.

General Order OPR 1.20

a. At the Area office, a separate file will be maintained for each LPR unit assigned to the Area. Each file will include all Monthly Plate Reader Activity Logs submitted after LPR system usage. These logs will be handled as Department-governed non-records (DGNRs) and shall be retained for two years after the end of the calendar year.

b. At the Division headquarters, all Monthly Plate Reader Activity Logs will be reviewed by the Division LPR Coordinator and consolidated into one Monthly Plate Reader Activity Report. The report shall be reviewed by the Division Commander and forwarded to the Statewide LPR Program Coordinator by the 5th of each month. The Division is the record holder for the Monthly Plate Reader Activity Reports, and these reports shall be included on the Division's file list. Monthly Plate Reader Activity Reports shall be retained for two years after the end of the calendar year.

Data Security and Access

13. The Statewide LPR Program Coordinator is responsible for overall operations of the program, including:

    a. controlling access of sworn personnel to the LPR system and hot file data;

    b. ensuring stored data are purged from the LPR system server as required;

    c. approving or denying in writing requests to access and/or use LPR data; and,

    d. designating personnel who will be authorized to access the server and conduct data queries.

14. The Department's Data Center will house the Department's LPR System Operations Center, which is the central database for all license plates scanned by the Department's LPR units.

    a. All collected data will be maintained on an independent server that is not connected to, or shared with, other law enforcement databases.

    b. The Data Center will provide an inquiry tool, history tracking, and reporting protocols for the entire LPR program.

    c. The Data Center will provide a secure intranet site, allowing only approved personnel password-protected access to collected data. This access shall be restricted to:

(1) searching for a license plate or partial license plate;

(2) viewing the image and location of matches on the "hot list";

(3) viewing maps showing the location of alarms or hits;

(4) viewing statistical reports on alarms or hits; and,

(5) searching for matches for a specific geographical location and/or time frame.

Operator Training

15. All users must receive standardized training prior to operating the LPR system.

a. The Statewide LPR Program Coordinator is responsible for providing initial training of all Department personnel who utilize the LPR system.

b. Additional training will be provided as needed and as determined by the Statewide LPR Program Coordinator.

c. The Training Division will be responsible for maintaining and updated all training records associated with the LPR program.

Data Storage and Retention

16. Per the Virginia Attorney General's Opinion #12-073, "License Plate Readers – Use and Storage of Data," the Department may not passively collect and store plate read data for potential use in future investigations.

a. The collection and use of stored data to help solve future crime are prohibited under the Opinion and existing Virginia law.

b. The Department may continue to use the LPRs to compare active reads to existing lists, such as stolen vehicles or Amber Alerts. Only the reads that are directly related to the intended purpose (i.e., stolen plate) may be retained beyond the use session of the LPR. All other non-relevant, passive reads should be deleted at the end of that day's use.

c. The Department may collect, store, and analyze data that relates to a specific, on-going, active investigation. That data shall be made part of the criminal investigative file and may not be used for other purposes.

General Order OPR 1.20

d. The Department may collect and temporarily store data that relates to special events as enumerated in paragraphs 10 and 11 of this General Order. This data will only be stored during the event and will be disposed of immediately following the event if it has been determined no applicable criminal investigation has been initiated. If an applicable criminal investigation is initiated, the data will be handled in accordance with paragraph 16.c. of this General Order.

Appendix D AAMVA License Plate Reader Working Group Roster

CHAIR AND LAW ENFORCEMENT REPRESENTATIVE

Captain Matthew Beaudin
Colorado State Patrol

LAW ENFORCEMENT REPRESENTATIVES

First Sergeant Robert Alessi
Virginia State Police

Lieutenant Chris LaPrairie
Nevada Highway Patrol

Captain Joseph Moody
North Carolina Department of Motor Vehicles
License & Theft Bureau

Colonel Allan Shinney
Utah State Tax Commission

Sergeant Jonathan Zarkauskas
Virginia State Police

MVA REPRESENTATIVES

Betty Johnson
Division Administrator
Nebraska Department of Motor Vehicles

Rosa Yaeger
Director
South Dakota Department of Revenue

IACP REPRESENTATIVE (MEMBER)

Major Josh Swindell
Ohio State Highway Patrol

IACP REPRESENTATIVE (STAFF)

Ryan Daugirda
International Association of Chiefs of Police

TECHNICAL ADVISORS

Dennis Bernardo D'Annunzio
Firmware and Software Development Manager
Leonardo

Jeff Hielsberg
Regional Sales Director
Intellectual Technology, Inc.

Kyle Hoertsch
Vice President of Public Safety Client Relations
Motorola Solutions

Steve Vaughn
Vice President of Field Operations
PrePass Safety Alliance

Mark Muriello
Director, Policy & Government Affairs
International Bridge, Tunnel and Turnpike Association

AAMVA STAFF – PROJECT MANAGER

Brian Ursino
Director, Law Enforcement Programs
American Association of Motor Vehicle Administrators

AAMVA STAFF

Paul Steier
Director, Vehicle Programs
American Association of Motor Vehicle Administrators

OUR VISION

Safe drivers
Safe vehicles
Secure identities
Saving lives!

AAMVA

American Association of Motor Vehicle Administrators
4401 Wilson Blvd, Suite 700
Arlington, Virginia 22203
703.522.4200 | **aamva.org**


MASSACHUSETTS
STATE
POLICE
MASSACHUSETTS
STATE POLICE
ALPR

ALPR Saves Lives!

Recent successful uses:

- AMBER alert and reported child abduction
- Mass shootings and multiple homicides
- Recovery of a missing/endangered elderly male
- Human trafficking investigation involving juveniles
- Catalytic convertor theft ring
- Fatal hit & run of bicyclist
- Fugitive wanted for attempted murder & sexual assault
- Arson with injuries
- Bank robbery pattern
- Armed home invasion

Terminology

- *Automatic License Plate Recognition (ALPR)*: AKA Automated License Plate Reader; cameras capture images of license plates and computer algorithms such as Optical Character Recognition (OCR) to convert the images to readable text data.

- *Read:* A scan of a license plate observed by an ALPR camera.

- *Hit*: A match between a license plate observed by an ALPR camera and a record maintained on a Hot List.

- *Hot List*: License plate numbers of vehicles of interest, such as vehicles associated with missing or endangered persons, AMBER & Silver alerts, kidnappings, wanted fugitives, including vehicles which are the subject of ongoing public safety or criminal investigations.

ALPR in 2023

- Nationwide trends
- Judicial/legislative trends
- Comm. v. McCarthy (2020)
- Exigent vs. investigative use



2753

Effective Date:	Number:
June 27, 2023	**TRF-11**
Subject: **Automatic License Plate Recognition**	

Policy

- Review policy (provided and available in PowerDMS)
- Authorized and unauthorized uses detailed in TRF-11
- System queries are subject to review/audit
- Unauthorized use will result in loss of access & discipline

Searches

- Searches may have legal implications
- Geographic and temporal parameters
- Minimization & privacy considerations
- Watermark & time sync verification
- Data retained per DCJIS policy
- Data visibility may be further restricted
- Preserve or export records needed for case

Hot Lists

- Entries should include:
  - Vehicle description, if available
  - Case number or reference and justification
- Entries expire automatically
- Remove when no longer needed/valid
- Special attention to rentals and short-term use
- May require supervisor authorization, see TRF-11

Alert/Hit Confirmation

Before taking enforcement action from an alert:

Verify the plate:

- Visually verify that the plate matches the OCR interpretation;

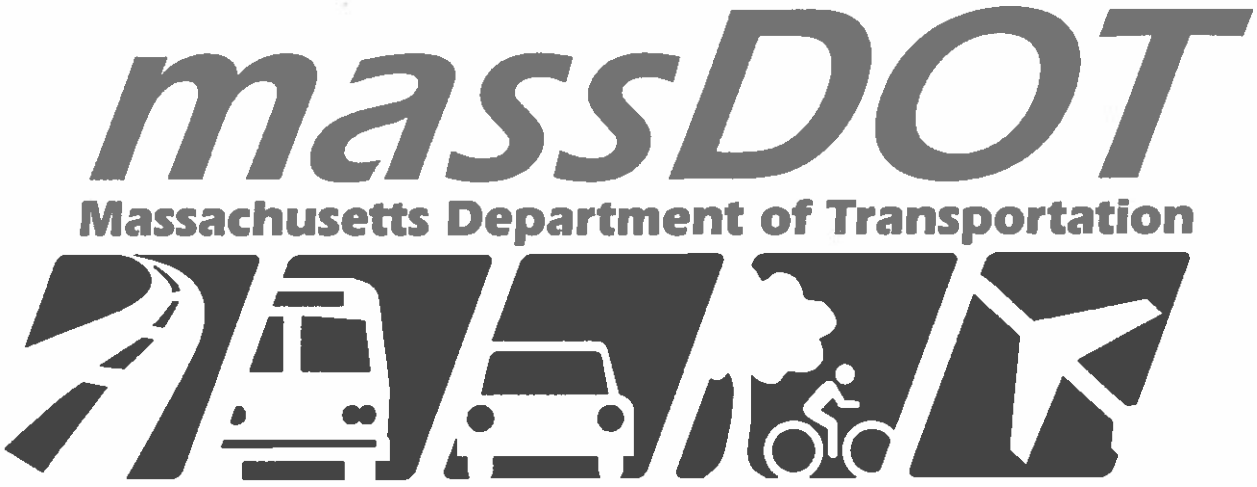
Verify the state:

- Visually verify that the state matches the Hot List information; and

Verify the status:

- Verify the current status of the plate (is the subject still wanted or vehicle still stolen?)


MASSACHUSETTS
STATE
POLICE



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**.~~

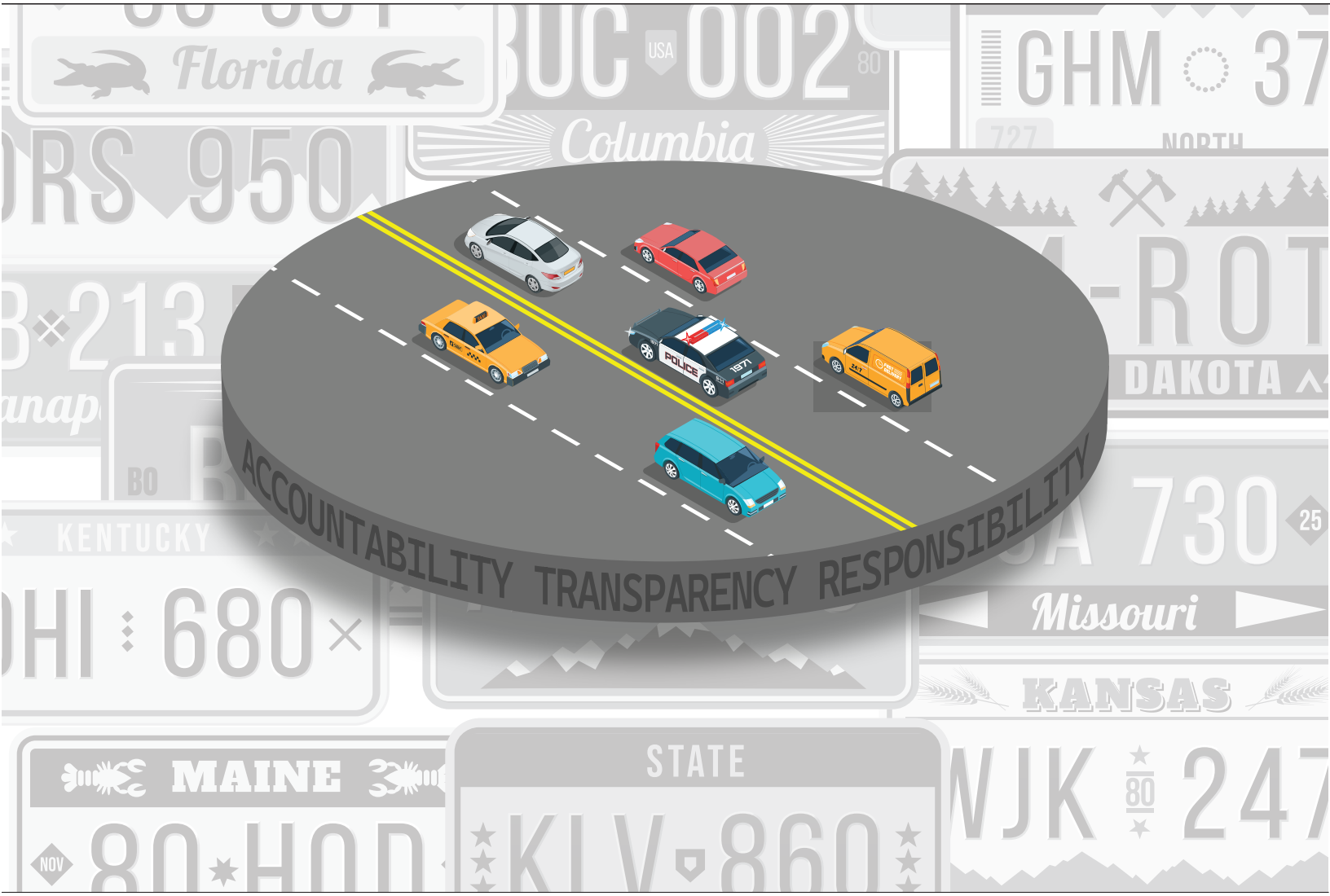
Any contracts resulting from this RFR may be used by **all departments of MassDOT**, the Commonwealth, including all constitutional offices, the legislature, and the judiciary; cities, towns, municipalities, counties, and other political subdivisions of the Commonwealth, including schools, and other 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

MAJOR CITIES CHIEFS ASSOCIATION

Automated License Plate Reader Technology in Law Enforcement

RECOMMENDATIONS AND CONSIDERATIONS



PRESENTED BY MCCA ALPR WORKING GROUP

2761

Table of Contents

Introduction — I
Executive Summary — II
Key Recommendations — III
Methodology of Product — IV
What is an Automated License Plate Reader? — 1
- ALPR Hardware and Software
- Types of ALPR
- The ALPR Detection Record
- Hotlist Sources
- Tactical vs. Investigative Uses
- Business/Private Use

Program Design and Development — 3
- Policy Development
- Training Considerations
- Deployment Strategies

Procurement — 7
- Vendor and Product Assessment
- Technical Challenges
- Procurement Ethics

Program Management and Oversight — 9
- Access and Appropriate Use
- Data Sharing
- Auditing, Data Collection, and Reporting

Data Stewardship — 13
- Data Roles and Responsibilities
- Data Security
- ALPR Reader Device Integrity

ALPR Operations Infographic — 15
ALPR Synergy with Other Law Enforcement Technologies — 16
- Beyond ALPR: AI-Enhanced Vehicle Detection

Case Law Related to ALPR — 17
- Privacy Expectations on Public Roadways
- Is ALPR Persistent Tracking?
- License Plates & Personally Identifiable Information (PII)
- Data Collection & Sharing
- ALPR Hits & Degrees of Intrusion

Conclusion — 21
Acknowledgments — 22
Definitions — 23
Appendix A – Success Stories — 24
Appendix B – Myths and Misconceptions — 26
Appendix C – State-Level Laws and Regulations — 28
Appendix D – CJIS Security Policy — 31
Appendix E – ALPR Audit and Transparency Report Template — 33

2762

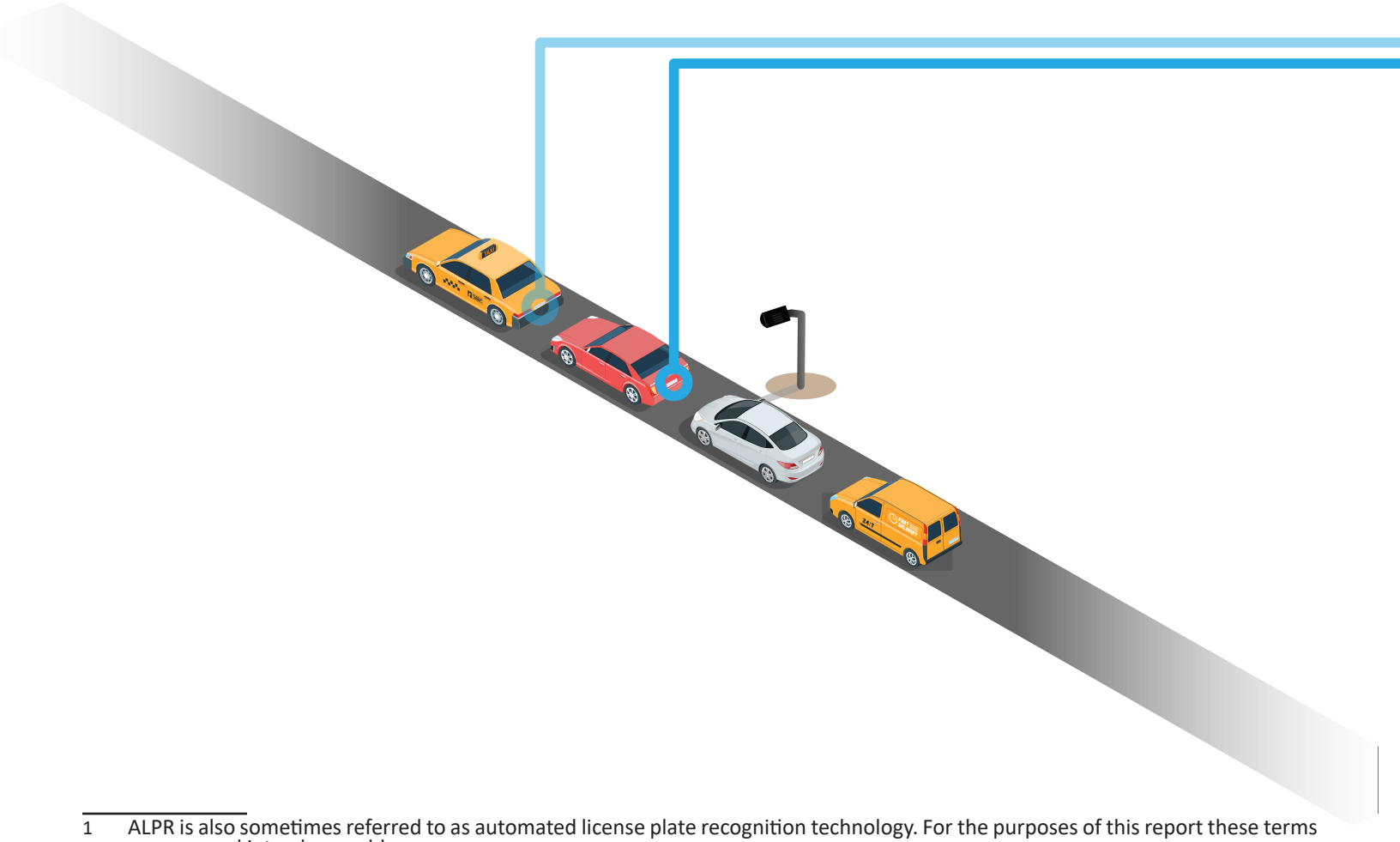
Introduction

Modern-day law enforcement relies on advanced technologies to enhance investigative capabilities. One example of these technologies is automated license plate reader (ALPR).[1] ALPR has been used for decades by law enforcement agencies throughout the United States, Canada, and across the globe to help generate leads and close cases. Law enforcement agencies that utilize ALPR continuously report that the technology is a critical tool that helps advance their efforts to fulfill law enforcement's ultimate mission of keeping our communities safe.

ALPR is a proven technology, but all law enforcement tools must be used ethically and appropriately. This product is designed to assist law enforcement agencies with developing and maintaining an ALPR program that respects citizens' Constitutional rights and privacy while maintaining ALPR's effectiveness as a tool to address crime.

In October 2022, the Major Cities Chiefs Association (MCCA) established an ALPR Working Group composed of trusted technology partners, law enforcement agency stakeholders, and subject matter experts in the ALPR field to achieve this goal. The Working Group has created a set of best practices related to procurement, development, operation, data collection and reporting, and other elements instrumental in creating a well-balanced ALPR program. Like any other technology, ALPR will continue to evolve.

The product is a true public-private partnership, and the framework outlined in it will help law enforcement agencies seeking to utilize ALPR achieve the highest possible standards. However, it is essential to remember that every community is different, and what works in one community may not work in another. Therefore, while the Working Group's recommendations provide a strong foundation, agencies are encouraged to tailor them to meet the specific needs of their community as they develop, implement, and manage their ALPR program.



1 ALPR is also sometimes referred to as automated license plate recognition technology. For the purposes of this report these terms are used interchangeably.

2763

Executive Summary

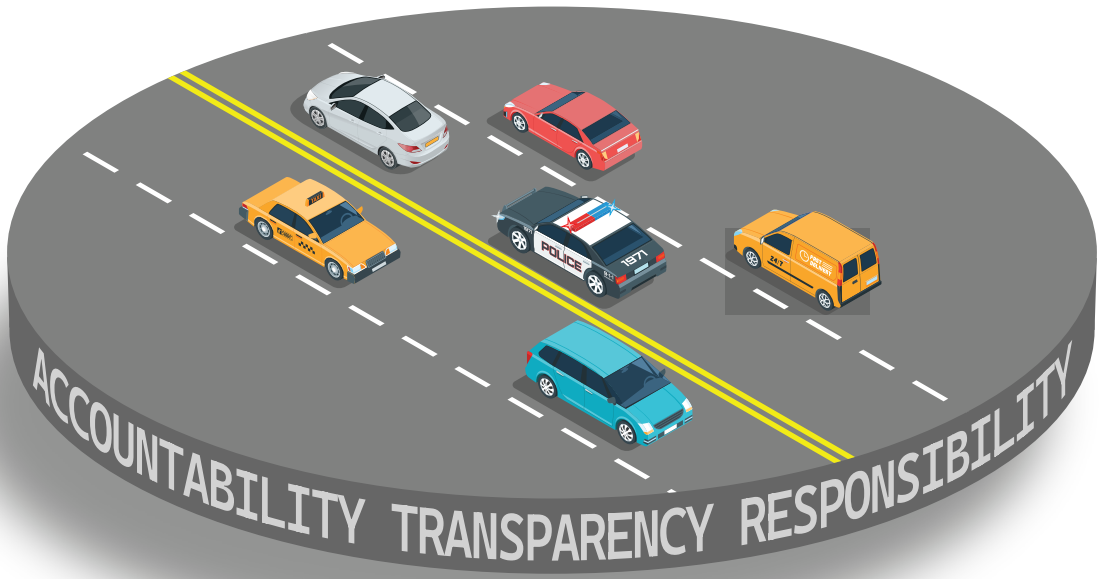
In October 2022, the Major Cities Chiefs Association (MCCA) launched an ALPR Working Group composed of trusted technology partners, law enforcement agency stakeholders, and subject matter experts. The Working Group has developed a product that is designed to provide MCCA members and other law enforcement agencies with guidance on developing, deploying, and responsibly using ALPR technology. ALPR technology has proven to be a powerful tool to combat criminal activity, generate actionable investigative leads, and help close cases faster.

This product directly addresses the most critical aspects of ALPR technology, which can be subdivided into three main categories: accountability, responsbility, and transparency. The product outlines suggestions on ALPR program design, policy development, training considerations, and deployment strategies. The product also covers ALPR procurement. Finally, it addresses the ongoing management and oversight of the technology and provides an overview of relevant case law. While these suggestions and recommendations address the most critical aspects of ALPR, they leave sufficient room for agencies to develop programs that meet their specific needs.

Stakeholders concerned about ALPR typically focus on disparity of impact, infringement of privacy, and the effects on individual rights. However, the Working Group strongly believes these concerns can be sufficiently addressed and mitigated through thoughtful policy design, effective management, and proper oversight. Furthermore, it is important to note that recent case law differentiates the capabilities ALPR provides from those of other law enforcement technologies.

The guidance outlined in this product serves as a template for building and operating an ALPR program that is both effective in its use and responsible in its nature. By implementing the Working Group's suggestions and recommendations, law enforcement agencies can ensure their ALPR programs are helping to keep communities safe while protecting citizens' privacy, civil liberties, and Constitutional rights. In addition, this can help increase public trust and build support for using ALPR technology.

Finally, like all technology, ALPR will continue to change and evolve. For this reason, this product should be considered a living document rather than a finalized template for developing and implementing a balanced and responsible ALPR program. As the conversation surrounding ALPR progresses, so will the recommendations and suggestions included in this product.



2764

Key Recommendations

The following key recommendations serve to highlight the MCCA ALPR Working Group's most essential recommendations and considerations. They have been grouped by their applicability to three foundational principles regarding the deployment of advanced technologies in law enforcement.

ACCOUNTABILITY

- Agencies should develop a training program that establishes accountability guidelines, procedures for responsible use, and emphasizes transparency. The use of ALPR technology should be limited to trained personnel.
- The use of ALPR technology should be limited to criminal investigations or to address an articulable public safety concern.
- The procedures for the use of ALPR technology should emphasize the need to confirm the accuracy of the information presented prior to taking enforcement action.
- Careful consideration should be given to the data retention policies implemented by the agency. Data retention time frames should be developed by balancing community needs, benefits, and concerns.
- Audits of ALPR programs should be conducted regularly. Audits should monitor user activity to ensure appropriate use in accordance with established policies.

RESPONSIBILITY

- Sharing ALPR data among law enforcement agencies can enhance the effectiveness of ALPR deployments. A clear policy should be established prior to enabling data sharing to address data usage and deconfliction requirements.
- Deployment strategies should be reviewed regularly and evaluated to ensure the ALPR program and technology continues to operate within the established objectives and policies.
- Law enforcement agencies seeking to procure ALPR technology should consult with other agencies that have deployed ALPR during program development.
- Prior to the deployment of ALPR technology, agencies should assess existing technological deployments and consider how they can complement or enhance their specific program strategy.
- Law enforcement agencies must implement strict cybersecurity protections to prevent unauthorized access of ALPR data.

TRANSPARENCY

- Deployment plans should be informed by analyzing crime data, patterns, and trends to ensure the technology is deployed in an equitable and responsible manner.
- Agencies should consult with their local public works and other relevant stakeholders to ensure the ALPR deployment plan meets all permitting, legal, and other requirements.
- Comprehensive data collection and reporting will help maximize the benefits of ALPR technology by increasing transparency and empowering agencies to determine its impact on crime and public safety.

2765

Methodology of Product

This product represents the comprehensive collection of the MCCA ALPR Working Group's recommendations and considerations regarding law enforcement's use of ALPR technology. The value of ALPR as a crime-fighting tool is well established. However, an effective program must include certain elements to ensure the technology is being used effectively and in a manner that maintains the trust and support of the community. This document will provide law enforcement agencies with a framework to develop, implement, and manage an ALPR program that is based on responsible use, helps keep the community safe, and respects privacy, civil rights, and civil liberties.

The MCCA ALPR Working Group includes technology vendors from various backgrounds, a diverse group of law enforcement professionals, and ALPR subject matter experts. In addition, the Working Group conducted in-depth research on ALPR technology from numerous perspectives. Finally, the Working Group leveraged the expertise of the individual participants to develop its recommendations and suggested best practices.

The information and data used to support the findings of this product include material provided by MCCA member agencies and technology vendors. The Working Group also reviewed products produced by other stakeholders on ALPR and the use of technology in policing more generally. Finally, the Working Group conducted regular internal discussions to finalize the recommendations and suggested best practices.

This product's outline and overarching topics were created collaboratively with input from all Working Group participants. Each participant was responsible for drafting a section of the report, and those drafts were circulated to the entire Working Group for review. All Working Group members approved the final product.

The final product represents the MCCA ALPR Working Group's findings, recommendations, and suggested best practices. These will help law enforcement agencies create, manage, and operate an effective and responsible ALPR program.

2766

What is an Automated License Plate Reader?

ALPR, called Automated Number Plate Recognition (ANPR) in Europe, was invented in 1976 by the Police Scientific Development Branch to combat terrorism in the United Kingdom. While seen as a valuable tool, the associated cost and requisite experience stagnated the deployment and advancement of the technology until the first ALPR cameras were installed at the Dartford Tunnel and A1 Road in 1981. The Dartford Tunnel cameras resulted in ALPR's first arrest for a stolen vehicle. This slowly led to more widespread use of the technology, including as part of the "ring of steel" created around London in the early 1990s to protect against the Irish Republican Army (IRA) bombing campaigns. Later, ALPR technology was also deployed as part of another initiative entitled "Project Laser," which sought to "target criminals through their use of roads."[1]

The success of the "ring of steel" and "Project Laser" prompted the Police Standards Unit to create the National ANPR Data Centre (NADC) in 1997. The NADC allowed for the nationwide sharing of ALPR data across the United Kingdom and the Back Office Facility (BOF), the database where ALPR data was stored and analyzed. ALPR technology took off from here. Law enforcement first used ALPR to help solve a murder case in 2005, and by 2007, nearly half of all law enforcement agencies in the UK were using ALPR technology. American law enforcement agencies followed their British counterparts closely and started using ALPR in 1998.[2]

ALPR Hardware and Software

While the technology has advanced over the years, the main components of those early ALPR deployments and today's systems remain the same. At its core, an ALPR program consists of the camera hardware and the software used to store and analyze the generated data and alert the users when a detection of interest is made. In most cases, ALPR hardware consists of a camera, processor, power supply, and data transfer hardware. In addition, ALPR cameras are typically optimized in various ways to operate in a wide range of real-world conditions (low light, inclement weather, motion detection, etc.).

Once the camera captures the image, ALPR systems use software to read the license plate. Some systems process the image at the camera level. Other systems transfer (usually via a cellular network, but it may occur through other means) data from the camera to a dedicated ALPR-system computer for processing. The image is analyzed through Optical Character Recognition (OCR) software as part of the processing. OCR recognizes alpha-numeric numbers and letters, thereby allowing the ALPR system to successfully recognize and interpret any letters or numbers observed in the image captured by the camera.

Types of ALPR

Law enforcement uses various types of ALPR technology, including fixed, mobile, portable, and mobile applications. Below is a description of each kind of ALPR system:

- **Fixed ALPR** cameras are typically permanently mounted to infrastructure such as traffic signals, bridges, and light poles.
- **Mobile ALPR** cameras are typically mounted on vehicles. These cameras may be overtly or covertly deployed depending on the needs of the law enforcement agency.
- **Portable ALPR** cameras include mobile camera trailers which can be transported and deployed based on the law enforcement agency's operational needs.
- **Mobile Applications** leverage features built into cellular devices to create ALPR detections.

1 David J. Roberts and Meghann Casanova, Automated License Plate Recognition (ALPR) Systems: Policy and Operational Guidance for Law Enforcement, National Institute of Justice, U.S. Department of Justice, 2012. https://www.ojp.gov/pdffiles1/nij/grants/239605.pdf

2 B.A. Reaves, Local police departments, 2013: Equipment and Technology. Bureau of Justice Statistics, U.S. Department of Justice, July 2015. https://bjs.ojp.gov/library/publications/local-police-departments-2013-equipment-and-technology

2767

The ALPR Detection Record

An ALPR record is generated when a vehicle license plate is detected, imaged, and processed to create a record. An individual ALPR record (or 'plate read') is generally composed of the following:

- An image of the license plate, which is a 'cropped' digital image of the license plate captured by the camera.
- The geo-location where the plate detection occurred, which can be determined from the GPS coordinates of a mobile reader or inferred from the location where fixed readers are placed.
- The time and date when the license plate detection occurred.
- The translated information from the plate, which is the alpha-numeric plate number and the issuing organization, typically a state. This translation can be accomplished by OCR or artificial intelligence.

In addition, an ALPR record may contain the following:

- A collateral image of the vehicle for which the ALPR read occurred.
- Metadata associated with the camera that identifies the camera unit, image settings, and other specific attributes.

Hotlist Sources

ALPR systems used by law enforcement can alert on detections of wanted vehicles. Two primary methods exist for creating a wanted vehicle within an ALPR system. First, ALPR systems allow for the manual entry of both a hotplate and a hotlist. Second, the ALPR system allows agencies to import National Crime Information Center (NCIC) records as an automated hotplate source. This is the most common method for populating hotlists.

Tactical vs. Investigative Uses

Law enforcement typically uses ALPR technology for both tactical and investigative purposes. Accordingly, agencies should consider both uses when developing their ALPR program's objectives. A tactical ALPR deployment includes placing cameras in strategically identified locations to generate information that warrants a rapid police response, such as stopping a wanted vehicle. These deployments usually seek to identify, locate, and recover a vehicle or its occupants to help address crime occurring in real time. An investigative use refers to utilizing ALPR cameras to collect license plate records that may have law enforcement interest but do not necessarily warrant an immediate police response. These detections are stored in the system and may later be queried. This information is generally used to create an investigative lead after a crime has occurred.

Business/Private Use

Since ALPR systems provide valuable data, private businesses and other organizations have also invested in ALPR technology. These uses may be for security, management, or operational needs. The following are examples of private sector use cases:

- Parking garages
- Hotels and casinos
- Homeowners associations
- Airports
- Convention centers
- Government traffic and transportation sites

2768

Program Design and Development

ALPR has proven to be a successful law enforcement tool. Its unique ability to provide actionable leads and help close cases cannot be overstated. However, real and perceived concerns exist regarding this technology's use. Therefore, law enforcement must take careful steps to develop an ALPR program that is both effective and appropriate. Taking a thoughtful approach when designing and developing these programs is the best strategy to accomplish these goals. Some of these considerations include developing proper policies, creating comprehensive training material, and designing and implementing responsible deployment strategies.

Policy Development

Establishing clearly defined policies on how ALPR may be used is the most effective method to minimize risk to the agency and protect both department employees and the individual rights of the public. ALPR policy should direct the purpose, general use, and processes involving ALPR investigations. These policies will provide a framework by which an agency can simultaneously reap the benefits of the technology, all while respecting the privacy and civil rights of the public. Similarly, consistent policies will assist in protecting the integrity of criminal investigations, criminal intelligence collection, and justice system processes. The following components should be considered while developing ALPR policies and procedures:

- Community-directed statement on why the agency is establishing or maintaining an ALPR capability
- The purpose of the policy
- General use guidelines of the technology
- Clearly defined program oversight roles and responsibilities
- The ALPR vendor and deployment types
- Access, training, and usage requirements
- Investigative procedure requirements
- Clear guidance to department employees on being transparent on the use and reporting of the technology in court documents
- Auditing responsibilities and schedule
- Data retention and purging
- Statement affirming protections for constitutionally protected activities
- Rules governing the use of hotplates

State/Local Law Considerations

Many state legislatures have taken steps to regulate the use of ALPR technology in their states. These laws and regulations can directly impact the functioning of an ALPR program in those states, and they must be accounted for in agency policy. Examples of the types of rules and regulations implemented in several states can be found in Appendix C – State-Level Laws and Regulations.

Training Considerations

Ensuring a thorough training program is in place is critical. Users must receive training on the ALPR system before receiving access. This practice ensures ALPR systems are only used for official law enforcement purposes consistent with applicable legal limitations and department policy. The training program should address several topics to ensure that users of an ALPR system are proficient in the necessary skills, including:

- A review of the departmental policy and safeguards related to ALPR use
- Basic understanding of how the technology operates
- The ALPR data sources, vendor, type of systems, etc.
- Any significant capabilities and or limitations related to the technology
- Any potential hazards related to the technology

2769

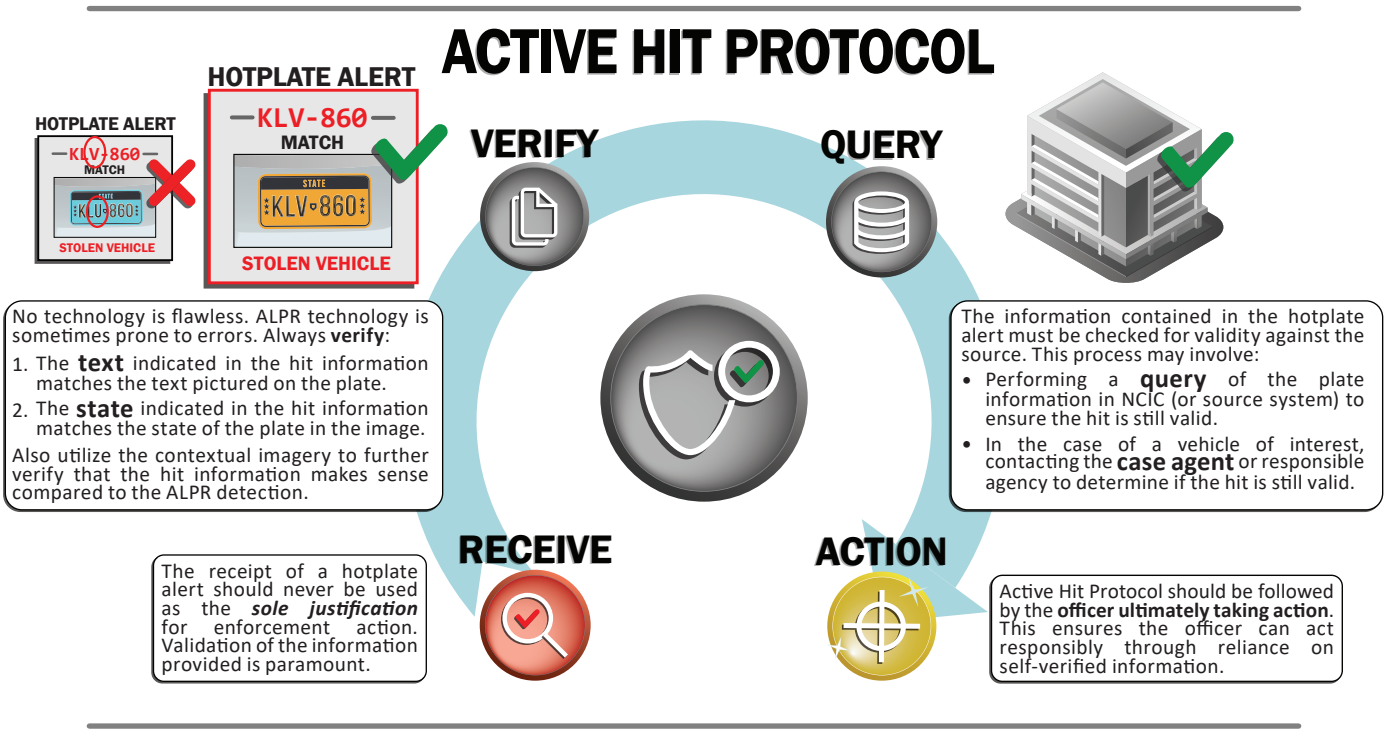
- Who is authorized to access the system and any required training
- The role of the officer or investigator in leveraging and responding to ALPR hotplate detections
- Importance of being transparent with arresting documentation
- Any applicable laws and policies that govern the use of ALPR in the specific jurisdiction
- Use of the ALPR system as an investigative tool
- The data retention period
- Auditing responsibilities

An ALPR training program should include a tactical-level discussion of how to use the technology appropriately. For mobile units, this should consist of an initial check to ensure that the ALPR system is operating correctly at the beginning of each shift. This includes logging into the system, running any necessary diagnostics to determine that it is working correctly, and doing a quick physical inspection of the system (cameras, cables, connections). In addition, a program manager should conduct periodic checks of fixed ALPR sites to verify that the hardware is operational and communicating with the software as intended.

Field Officer Responsibilities

A critical piece of the officer training on ALPR should include an element that instructs how ALPR notifications are processed and the appropriate response protocols for those notifications. Some departments may have fixed ALPR hits reviewed and confirmed by the public safety answering point or real-time crime center before dispatching them to an officer to investigate. Other systems may provide an in-car alert on the car computer system.

Officers should be required to review hotplate detection, confirm the detections, and appropriately respond to actively wanted vehicles. This process can be referred to as “Active Hit Protocol.”



2770

Investigator Responsibilities

The ALPR system is a valuable investigative tool. It can be used to develop leads in cases involving vehicles where the license plate is unknown or to establish that a car was not in the vicinity during the time frame a crime occurred. An ALPR training program must include how to access the system and the criteria required before conducting a query, such as the reason for the search and the associated case number. Additionally, investigative tool training should address how to query the system, instructions on operating the various analytical tools within the system, how to interpret the data, how to preserve a record, and any required transparency, audit, or reporting requirements.

Types of Training

Training should be broken down into multiple categories:

- **New User Training:** This training will be detailed and define proper usage. In addition, this training should include policy, procedures, state and local laws, and an in-depth walk-through of the ALPR products and software.
- **Refresher Training:** This is considered a refresher of policy and procedures. It may also include changes to case law and examples of ALPR use. This training should ideally occur immediately after any changes to policy take place.

Authorized instructors should provide training on ALPR technology based on an established, accredited curriculum. An example of an accredited curriculum is one that has been approved by the state's Peace Officer's Standards and Training (POST) or equivalent body.

Deployment Strategies

Determining the ALPR deployment type and kind is one of the most critical decisions an agency will make concerning its ALPR program. Law enforcement is responsible for deploying advanced technology in a manner that is effective in its use and appropriate in its scope. Law enforcement also has a fiduciary duty to use public funds responsibly. For these reasons, ample consideration should be made when determining the type and kind of ALPR deployment.

ALPR Deployment Theories

As previously addressed, various types of ALPR technology exist, including fixed, mobile, portable, and smartphone applications, with each serving a unique purpose. Therefore, the kind of ALPR selected should be determined by the environment, infrastructure, and objectives for the ALPR deployment. Several ALPR deployment strategies are often considered when determining the value and placement of ALPR cameras. The most common of these strategies include the following:

- **High Traffic Areas:** The primary objective is to collect the maximum number of detections that can later be leveraged for investigative leads.
- **High Crime Areas:** This strategy focuses on producing information anticipated to be of investigative value instead of creating as many detections as possible.
- **Places of Interest:** This strategy is more of a hybrid between the first two. An example of this strategy would be deploying ALPR cameras around a shopping mall targeted by organized retail theft gangs or where assaults have occurred. Agencies may also place ALPR cameras in proximity to their community's major ingress/egress points and critical infrastructure or routes associated with gun, drug, or human trafficking.

Deployment Considerations

Infrastructure and permitting are two common factors that can limit an agency's deployment strategy for ALPR systems. Agencies must carefully consider each physical deployment site. The infrastructure to mount the necessary hardware must exist for the technology to be successfully deployed. Furthermore, the owner and operator of the infrastructure or property must allow for the installation of ALPR hardware. Agencies must also ensure that the proposed site is appropriate for the type of power the ALPR utilizes. Some systems run on AC power. While this provides constant and consistent power, installing it can be more expensive. Others rely on solar energy, which may only provide enough power if the camera site receives sufficient sunlight to account for the traffic volume. Finally, this infrastructure must have access to a data transmission service, such as cellular, fiber optic, or Wi-Fi.

Once a deployment plan has been established, site locations have been determined, and in-person inspections of the sites have been completed, the agency will need to navigate any legal and permitting processes. Since permitting can vary significantly across jurisdictions, it is recommended that agencies consult with their local public works or other appropriate governmental entities to ensure all necessary procedures are being met. Engaging these entities earlier in the process will help secure their buy-in, which will be critical for a successful deployment.

Equitability Concerns

Deployment strategies must account for concerns over bias, surveillance or other threats to privacy, and potential chilling effects on First Amendment, defendant, or related rights. The following recommendations will help ensure ALPR technology is deployed in a manner that supports just and equitable policing:

- Deployment plans should be informed by analyzing crime data, patterns, and trends. The site selection process should be based on this information and account for any relevant privacy, equitability, or other concerns.
- Agencies should consult the community, other stakeholders, and appropriate oversight committees. This includes providing specific information on why and how the deployment sites were selected.
- Deployment strategies should regularly be reviewed and evaluated to ensure the ALPR program and technology continue s to operate within the established guidelines and policies.

Partner Technologies

While developing the deployment plan, it is important to consider other law enforcement technologies that may complement the ALPR system. Law enforcement agencies may deploy complementary technologies within the same area, which have different capabilities. Agencies can leverage these capabilities to increase their ability to suppress crime, create actionable leads, solve cases, and potentially deter future crimes. Potential partner technologies can be subdivided into two categories: tactical and investigative.

Tactical technologies include tools such as gunshot detection technology, public safety cameras, and drone detection technology. An example of investigative technology is a records management system (RMS). Integrating ALPR and RMS can join plate reads to hotlists, allow investigators to search plate reads within a familiar interface, and provide a direct link between case management and the ALPR database. Another example of investigative technology is crime analysis software. Bringing ALPR data into an agency's chosen analysis software can aid in ongoing investigations. For example, agencies can import ALPR data to help create accurate timelines for vehicle travel that can provide investigators with unseen leads and valuable knowledge.

2772

Procurement

Responsible procurement of ALPR technology is a critical component of an effective program. The importance of obtaining stakeholder feedback early in the procurement process cannot be understated. Program managers should make every effort to embrace a spirit of transparency, accept critical feedback, and attempt to address any concerns raised by stakeholders directly.

The procurement phase is also the appropriate time to begin building departmental policies, procedures, and protocols, as this will be crucial in gaining stakeholder buy-in. It is imperative that the stakeholders understand how these policies will protect the public's privacy and civil liberties. Agencies should also seek to mitigate any concerns that stakeholders raise about the proposed ALPR program through thoughtful policy design.

Vendor and Product Assessment

Before choosing a vendor for their ALPR program, law enforcement agencies should conduct an appropriate degree of market research. This should include a trial of the product and conversations with existing customers to evaluate its performance in a real-world setting. A trial period provides the opportunity to test the technology, the associated policies and procedures, and highlight initial successes. This can provide tangible examples that can be shared with stakeholders to show how ALPR serves to enhance public safety.

Should an agency engage in a pilot program, it is recommended that the community be notified. Agencies should also determine how any information collected may be used in investigations or other law enforcement operations until a final protocol and all other areas of the program are formalized.

When determining the best hardware for their ALPR program, law enforcement agencies should consider the following:

- Hardware requirements for specific sites
- The lenses, processor, and other technical specifications of the hardware
- Average detections per hour
- General cost
- The number of lanes of traffic a single camera can capture
- The maximum speed at which the camera can read a license plate

When determining the best software for their ALPR program, law enforcement agencies should consider the following:

- The accuracy of the OCR software and whether it's enhanced by artificial intelligence, machine learning, or another capability
- The technology's alerting system, including desktop, laptop, mobile, app-based, and in-car alerts
- The software's ability to connect and share data with other law enforcement analytical platforms

Technical Challenges

There are some challenges with ALPR software that agencies must acknowledge. For example, OCR technology analyzes all letter or number sequences in the imagery; it cannot specifically isolate only license plate images. Therefore, a detection can be created on something that is not a license plate. This includes billboards, signage, marketing material on vehicles, etc. Additionally, the full license plate letter and number sequence must be visible to create an accurate license plate detection. Occlusion, missing plates, and temporary paper plates may result in no detection, a partial detection, or a misread.

Misreads may occur for several reasons, but most are due to the incorrect translation of a letter or number. For example, the system may read an "8" as a "B" or a "K" as an "X." These technical challenges should be readily acknowledged by both the agency and a prospective ALPR vendor. Agencies must ensure their policies account for these challenges and contain sufficient safeguards to limit instances where officers act based on a misread or other error.

2773

Procurement Ethics

While local procurement ordinances vary across jurisdictions, agencies must follow those ordinances along with broader guiding principles when procuring an ALPR platform. The National Institute of Governmental Purchasing's (NIGP) Values and Guiding Principles of Public Procurement are one such set of broad principles that agencies can use to inform any ALPR procurement process. The NIGP principles are as follows:

- **Accountability:** Taking ownership and being responsible to all stakeholders for our actions. This value is essential to preserve public trust and protect the public interest.
- **Ethics:** Doing the right thing. This value is essential to deserve the public's trust.
- **Impartiality:** Unbiased decision-making and actions. This value is essential to ensure fairness for the public good.
- **Professionalism:** Upholding high standards of job performance and ethical behavior. This value is essential to balance diverse public interests.
- **Service:** Obligation to assist stakeholders. This value is essential to support the public good.
- **Transparency:** Easily accessible and understandable policies and processes. This value is essential to demonstrate the responsible use of public funds.[3]

3 Additional information on NIGP's Guiding Principles can be found here: https://www.nigp.org/our-profession/values-and-guiding-principles-of-public-procurement

2774

Program Management and Oversight

An ALPR program's design and operational management are part of the framework of a successful program. Effective management and oversight of the program help ensure operational transparency and accountability and that ALPR technology is being used responsibly.

To ensure the program operates responsibly, agencies should assign a manager operational control of the ALPR program. This individual should be well versed in the technology, have a sound understanding of all significant components of the ALPR program, and be empowered to ensure the program follows protocols, policy, applicable law, and community and agency expectations.

A program manager's responsibilities include the following:

- Developing policies
- Overseeing training
- Ensuring appropriate use of the technology
- Managing data collection and reporting

A program manager is also responsible for staying current on technology changes and emerging ALPR trends. Similarly, they must ensure that their agency's ALPR policies and training are current and address technological changes or advancements. Finally, having a program manager establishes a clear point of contact between the law enforcement agency and the ALPR vendor. This can enhance the communication between the agency and vendor, which creates an opportunity to share and address any technological or other challenges.

Access and Appropriate Use

Law enforcement agencies are responsible for using ALPR data to uphold public safety, solve crimes, and prevent future crimes. Agencies have an opportunity to build public trust and support for the use of ALPR through transparency and responsible use. As such, agencies should carefully consider the circumstances under which using ALPR is appropriate and what personnel within the agency can access this tool.

Law enforcement agencies must scope their ALPR programs in a manner that ensures the agency is still able to conduct proper oversight and operate the program transparently. One method for achieving this is by limiting who can access the ALPR technology. For example, many law enforcement agencies restrict access to specialized personnel to ensure that the use of ALPR technology is adequately audited and controlled. Access should only be authorized once a user has completed the requisite training and demonstrates a baseline understanding and operational knowledge of the technology. Information on new user training, access, and use should be part of standard data collection and reporting related to the ALPR program.

Agencies that deploy ALPR must have written policies that outline the appropriate use of the technology. Several core principles should be incorporated into these policies to ensure the responsible use of the technology. First and foremost, ALPR technology should only be used as part of a criminal investigation or to address an articulable public safety concern. Secondly, the investigator must also have a legitimate "need to know" before querying any ALPR data. These guardrails will help prevent "curiosity checks" or other bad faith uses and ensure that privacy, civil rights, and civil liberties are respected.

Agency users must also demonstrate adherence to established policies when searching archived ALPR data. For example, if the ALPR software allows it, agency policy should require users to document the investigative purpose and case number associated with each query. Vague or ambiguous reasons for a search, such as "criminal subject" or "research," should be avoided. An agency's ALPR policies should also outline the potential consequences and corrective methods for improper use of the technology. Examples may include mandatory retraining, loss of access privileges, or other appropriate corrective punishments.

Data Retention

Data retention policies are ultimately determined by the agency using ALPR technology. These policies are informed by various considerations, including the agency's objectives, stakeholders' expectations, and local laws or regulations. Therefore, it is essential that the ALPR technology, vendor, and any other relevant service providers support the agency's policies on retention.

While a general best practice is not to retain data any longer than is necessary, what constitutes "no longer than necessary" is not a simple determination since different use cases may benefit from different retention periods. For example, cold cases may benefit from years-old data, while other uses rely on more recent data.

Outside of specified legal requirements, the retention schedule for ALPR data is primarily determined by agency policy.[4] As such, law enforcement must work with the community and other stakeholders to determine appropriate retention periods for each type of ALPR data. Ideally, ALPR systems should allow agencies to define retention schedules and automatically purge any record not designated for retention by a registered user. In addition, regular system audits ensure retention standards are followed and instill confidence that system data is utilized appropriately.

Data Sharing

For good reason, law enforcement agencies worldwide are embracing ALPR technology. A 2013 Bureau of Justice Statistics study showed that 77% of agencies serving populations of 100,000 or more have access to ALPR technology.[5] Moreover, given ALPR technology's value to a single jurisdiction, law enforcement has begun to explore sharing ALPR data across jurisdictional boundaries. Sharing ALPR data amongst law enforcement agencies fosters a more collaborative approach to addressing public safety concerns across jurisdictional boundaries.

Benefits of Data Sharing

When law enforcement agencies share ALPR data across jurisdictions, the technology can provide more comprehensive data. A shared system creates more unified and robust coverage throughout a region. Several ALPR vendors currently provide their law enforcement customer base with the ability to share data with other law enforcement customers. The potential to cross-reference information between separate ALPR systems allows law enforcement to enhance their investigative capabilities and can reveal elements of illegal activity that may otherwise be unknown to the investigating agency. Several elements of ALPR data and systems can be shared, including the ALPR detections and user-created hotlists. Some ALPR vendors also allow agencies to establish data-sharing relationships between their products and other technology systems.

As a standard practice, law enforcement agencies should consider sharing ALPR data with one another to the extent that state or local laws and regulations permit. Agency policy should define what, if any, type of data sharing is in place, who is authorized to establish data-sharing relationships, and any procedures that govern the sharing of ALPR data. These procedures and data-handling agreements should be implemented in policy for both the sharing and receiving agencies.

The success of ALPR technology among law enforcement has led non-government entities to acquire the same technology. This includes retailers, property managers, towing and repossession companies, parking lot operators, homeowner associations (HOAs), and even individual households. Since the generated data is of the same format and often targets issues of mutual interest, ALPR vendors have created Public-Private Partnership (PPP) friendly user interfaces. These programs typically allow the unidirectional sharing of ALPR data from the non-government side to the law enforcement side only. These partnerships strengthen community relationships and ensure public investments are used responsibly.

4 David J. Roberts and Meghann Casanova, Automated License Plate Recognition (ALPR) Systems: Policy and Operational Guidance for Law Enforcement, National Institute of Justice, U.S. Department of Justice, 2012. https://www.ojp.gov/pdffiles1/nij/grants/239605.pdf

5 B.A. Reaves, Local police departments, 2013: Equipment and Technology. Bureau of Justice Statistics, U.S. Department of Justice, July 2015. https://bjs.ojp.gov/library/publications/local-police-departments-2013-equipment-and-technology

2776

Data Sharing Considerations

While data sharing benefits agencies, safeguards are needed to protect the agency that generates and owns the data. Data sharing guidelines can be specific to the type of shared data. For instance, if agency "A" shares ALPR detection data with agency "B," there may be no requirement for a formal agreement. In contrast, if agency "A" shares hotplates or agency-generated hotlists with agency "B," this scenario may require a formal agreement. This is because hotplates or hotlists are typically generated from a criminal investigation or law enforcement process or function that may require an officer to take action if there is a confirmed detection. Furthermore, the agency that receives the information should bear the responsibility and liability for their officers' actions in response to an alert.

Law enforcement agencies seeking to share or receive ALPR data must be aware of applicable federal, state, and local laws. As such, agencies should consult with their legal representatives to identify pending, proposed, or existing laws that may be relevant. For example, legislation is proposed annually at all levels of government which, if enacted, could limit law enforcement data sharing. Finally, agencies must consider any concerns from the community or other stakeholders before establishing multi-jurisdictional data-sharing relationships.

Auditing, Data Collection, and Reporting

Auditing and reporting an agency's use of ALPR technology is a critical component of a transparent and accountable ALPR program. The failure to operate a program in this manner will only exacerbate concerns related to misuse or contribute to the perception that ALPR technology is synonymous with increased surveillance. This will undoubtedly negatively impact police-community relations. Agencies should develop robust mechanisms to evaluate the efficacy of the technology and ensure it is being used appropriately.

Auditing Requirements

Regular audits on an ALPR system are one method for validating compliance with agency policies and applicable laws and regulations. As with other reporting requirements, the specific auditing measures, and the frequency of said audits, should be clearly defined in the ALPR program's governance documents. In general, audits should verify what ALPR information was accessed and by whom, in order to identify any improper or unauthorized uses of this data. Audits should also ensure that data within the system is being handled per agency policy, including information sharing agreements. They should also confirm that data is being purged as required under any applicable data retention schedules.

Data Collection and Reporting Considerations

Studies have shown that ALPR technology is most effective when used systematically and when deployment sites are strategically selected.[6] In addition, comprehensive data collection and reporting will assist agencies with maximizing the benefits of ALPR technology. Finally, robust data collection and reporting will help increase transparency.

At a minimum, agencies using ALPR should collect and report the following information:

- Number of detections
- Number of hotplate hits
- Number of queries conducted by users
- Number of arrests directly attributed to ALPR hotplate detections
- Number of user-generated hotplates
- Breakdown of hotplate hit types
- Year-over-year analysis and trends

By analyzing this data, agency leaders and stakeholders can determine whether their ALPR system is meeting deployment goals and has significantly impacted crime or other areas of police operations. ALPR data collection and reporting also provide valuable insight into ALPR system adoption throughout the organization.

6 C. S. Koper and C. Lum, "The impacts of large-scale license plate reader deployment on criminal investigations," Police Quarterly, 22(3), 305–329, 2019. https://doi.org/10.1177/1098611119828039

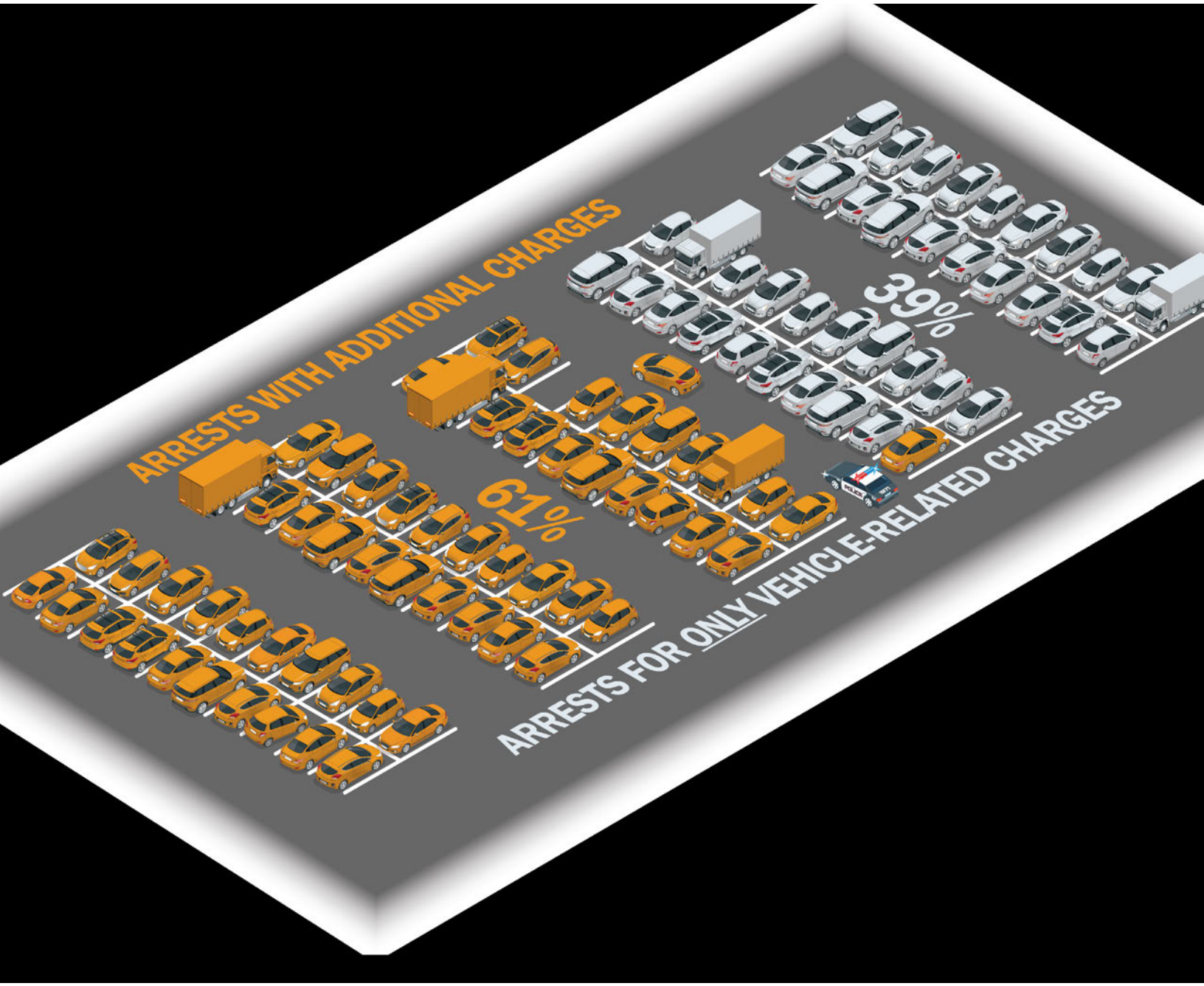
2777

The Importance of Analysis and Reporting

Quantitative data is an excellent tool to measure the impact of law enforcement technology. The ability to answer the questions “how many” and “how often” is necessary to evaluate real-world outcomes. Additionally, the quantitative analysis of ALPR data can provide an agency and stakeholders with the information needed to determine the impact of the technology on community safety.

To explore the potential of quantitative reporting, an MCCA member agency recently analyzed the impact of a localized ALPR deployment. The data presented below represents a period of four months after the installation of ALPR cameras within the evaluated area. The types of charges related to any arrests resulting from an ALPR event were analyzed. The data suggests that ALPR technology generates leads and solves more types of crimes than those related to ALPR’s most frequent use: the recovery of stolen vehicles.

It is important to capture and analyze the impact of any ALPR program to dispel misconceptions and demonstrate the impact of the technology.



2778

Data Stewardship

Throughout the design of an ALPR program, the hardware, software, and policies implemented will shape how ALPR data is collected and stored. Therefore, a comprehensive strategy should be developed to ensure all data collection aspects are secured and managed effectively.

Data Roles and Responsibilities

ALPR records are typically stored in databases that can be indexed, searched by individual or composite conditions, and analytically processed by applications that power ALPR use cases. This is an important and powerful compilation of data that must be managed judiciously. The two primary roles relative to this data are data owners and service providers.

The data owner is the organization that controls the data and decision-making authority. The data owner, typically the data's generator and user, determines how the data may be used, who it can be shared with, and its retention limits. For example, law enforcement is always the data owner for the ALPR data it generates. While this data may be shared with other law enforcement entities, the owner and provider of any particular data always retains control over all aspects of it. Therefore, other organizations that have received access to that data must act in accordance with the data owner's direction, such as adhering to retention limits established by the owner on the data.

A service provider is an entity that may take possession of data to store or process it on behalf of the data owner. The service provider operates at the behest of the data owner and enacts the owner's wishes and directions. This can include management of data sharing with other designated users, enforcing retention limits, etc. The service provider has no entitlement to the data and may not sell, derive secondary insights, or otherwise share it. Furthermore, they may only access the data to perform a function at the direction of the data owner. Law enforcement agencies often hire an outside company to be their service provider for ALPR data.

Storing and Processing ALPR Data

There are several general models for storing and processing ALPR data:

- The data is stored on-premises and processed by applications under the direct physical control of the organization that generates and uses the data.
- The data is stored off-premises by a cloud service provider and processed by applications in the cloud or on-premises under the direct control of the organization that generates and uses the data.
- The data is stored in the cloud or at an off site data center and is processed by a service provider.

In the first model, the data owner is effectively their own service provider, and there isn't necessarily a third party service-providing entity. The other two models imply some degree of a third party service provider. In those cases, the data may be held or accessed by another entity on behalf of the data owner. For ALPR systems, this could be either a cloud computing service or an ALPR technology vendor. However, in both cases, control of the data remains with the data owner.

Data Security

Law enforcement agencies should treat ALPR data like any other sensitive data it collects, uses, and manages. It should be protected as judiciously as law enforcement records, video, and other critical operational data. This includes ensuring responsible usage of the data by law enforcement personnel and vetting any service providers that may process the data. Law enforcement agencies must also apply rigorous cybersecurity practices to protect and secure the ALPR data it generates and uses. This includes, but is not limited to, proper authentication methods (multi-factor authentication is generally considered a best practice), data-sharing controls, and role-based access controls for users. Law enforcement agencies must ensure that their technology vendors provide adequate security practices to protect the ALPR data they possess and process on behalf of the agency.

2779
Whether a service provider provides on-premise technology, stores data on behalf of a law enforcement agency, or hosts the processing applications, they have an important role in ensuring the secure and trustworthy operation of an ALPR program. The service provider is responsible for securing the data it processes to protect it from unauthorized access, theft, or misuse. They must provide the necessary capabilities, controls, and training to enable law enforcement agencies to enforce their own defined data governance policies, security standards, and procedures. This includes:

- **Enforcement of Retention Limits:** This may be applied absolutely or in a role-based fashion. For example, the absolute retention limit for ALPR data could be three years, but only cold case investigators may access data older than six months.
- **Positive Controls Over How Data is Shared:** Data must only be shared after law enforcement specifically enables it with individual partners at its discretion and under the auspices of its policies.
- **Enforcement of Personnel Controls:** These controls include system and user-level authorization, role-based access controls, and regular audits.

The FBI's Criminal Justice Information Services (CJIS) Security Policy provides a comprehensive reference and standard that agencies may use to design or measure data management for their program. For cases where service providers take possession of ALPR data from law enforcement agencies to store and process on their behalf, agencies should consider using the CJIS Security Policy to assess and set expectations of service providers.[7] An explanation of relevant sections of the CJIS Security Policy can be found in Appendix D – CJIS Security Policy.

As mentioned earlier, cloud services may be part of an agency's ALPR program. These services' security and integrity depend on the efficacy of the underlying cloud platform. Cloud service providers (or service providers that operate their own data center directly) should comply with ISO 9001:2015, an internationally recognized standard for Quality Management Systems. Compliance with this standard should be independently audited and verified for compliance under the Statement of Auditing Standards Number 70 [SOC 2 Report]. In addition, compliance with FedRAMP medium security controls provides an additional level of validation and may be required for information sharing with federal entities. Even though license plate detection records are not personally identifiable, they may be linked through other sources that may enable the end user to input data that could be viewed as personally identifiable or criminal justice information.

ALPR Reader Device Integrity

An ALPR reader that captures ALPR images and does local image processing contains instances of ALPR data. This data may be transient or stored on the device for extended periods. Since ALPR readers are often distributed in the environment and may be difficult to physically secure, it is increasingly important to consider the device's ability to locally secure ALPR data that is either at rest or in motion. FIPS (Federal Information Processing Standards) 140 standards are used to evaluate the hardware and software integrity of cryptographic modules. This applies to many devices, including ALPR readers, that need to encrypt data to secure it from compromise. FIPS 140-2 is broken into four, successively increasing levels of security.[8]

- FIPS 140-2 Level 1 is the lowest and imposes limited requirements.
- FIPS 140-2 Level 2 adds requirements for physical tamper-evidence and role-based authentication.
- FIPS 140-2 Level 3 adds requirements for physical tamper-resistance (making it difficult for attackers to gain access to the sensitive information contained in the module) and identity-based authentication, and for a physical or logical separation between the interfaces by which "critical security parameters" enter and leave the module, and its other interfaces.
- FIPS 140-2 Level 4 makes the physical security requirements more stringent and requires robustness against environmental attacks.

Depending upon the specific environment where it is deployed, the ALPR reading device should, at a minimum, support FIPS 140-2 Level 2. Aspects of FIPS 140-2 Level 3 are also becoming increasingly desirable and necessary, especially as ALPR technology advances.

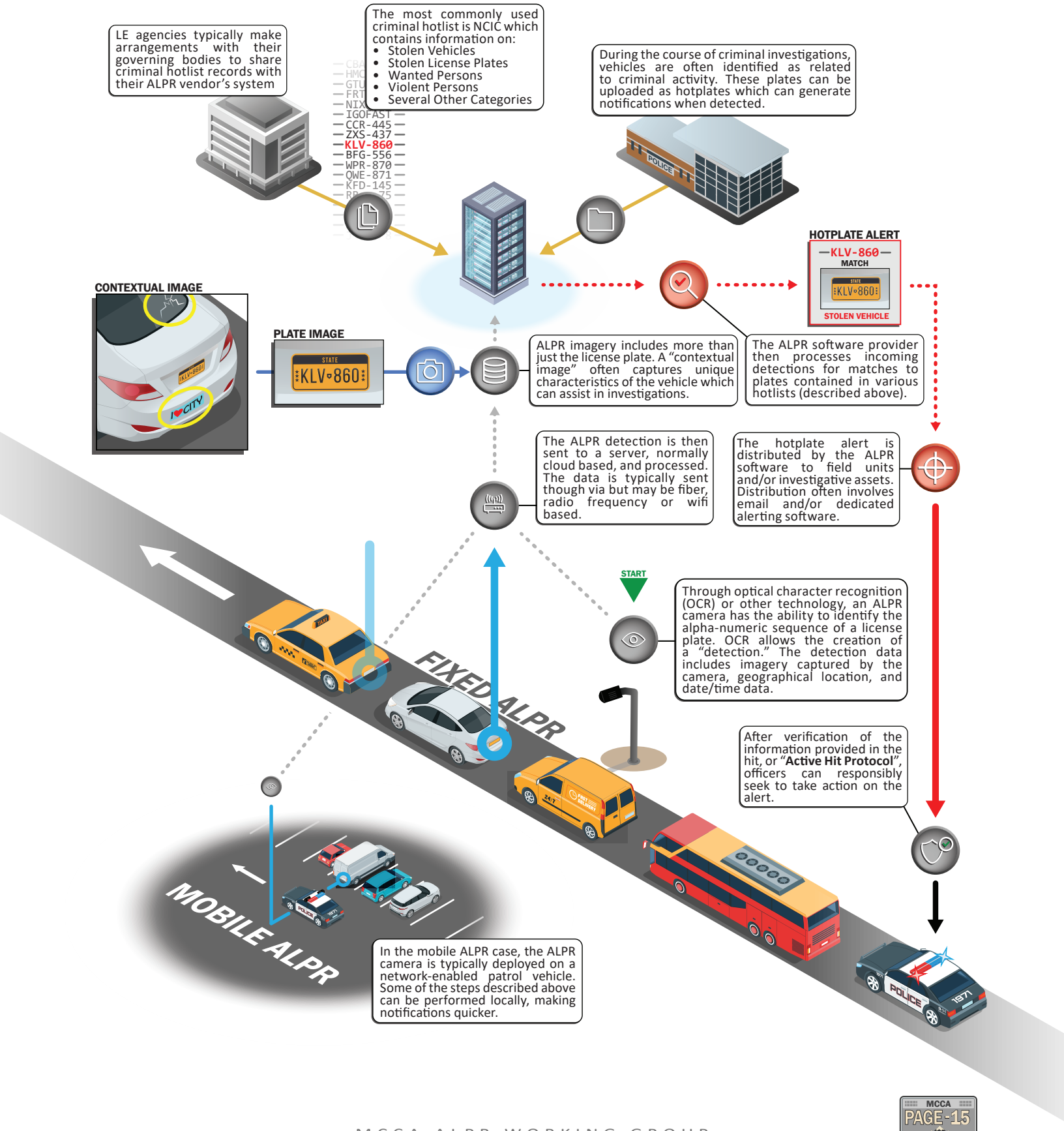
7 Criminal Justice Information Services (CJIS) Security Policy, CJISD-ITS-DOC-08140-5.9.1, US Department of Justice - Federal Bureau of Investigation, Version 5.9.1, October 22, 2022.

8 A. Lee, M. Smid, S. Snouffer, Security Requirements for Cryptographic Modules [includes Change Notices as of 12/3/2002], (NIST FIPS), National Institute of Standards and Technology, 2001. https://doi.org/10.6028/NIST.FIPS.140-2

2780

ALPR Operations Infographic

Several aspects of the operation of ALPR technology can be better understood when put in the context of the technological workflow.



2781

ALPR Synergy with Other Law Enforcement Technologies

As law enforcement gains access to more information, technology will help ensure the data is organized so law enforcement officers can solve complex policing problems. Any single data source, such as ALPR, only answers one of many questions. It only tells law enforcement where a vehicle was at a given time. ALPR alone does not answer critical questions such as whom the car belongs to or who has been associated with it before, whether any of those individuals have a history of involvement in similar incidents, and other critical questions.

By integrating data across common law enforcement data sources, those questions can be asked and answered immediately, drastically increasing the odds of solving cases. Here are a few examples:

> *Consider a situation where CCTV footage captures a partial plate on a vehicle shortly after the commission of a crime. In an ideal scenario, an ALPR database may be queried to determine the rest of the characters on the license plate. Then a separate RMS system could be queried to determine if that license plate has ever been mentioned in a case report.*
>
> *A platform has ALPR, RMS, citation, and crash data integrated into one place. An ALPR detection can be searched and then linked to see if that plate has been named in an RMS case, vehicle citation, or crash report, along with any involved individuals. Links between vehicles, people, and incidents can be seen without having to search each database individually.*
>
> *An ALPR alert occurs in a platform that has CAD & CCTV integrated. As a result, an immediate CAD call can be created to accompany the alert, and any relevant CCTV footage in the area can be attached and sent to the responding officer, better preparing them to engage with the vehicle that triggered the alert.*

In these examples, a singular piece of information would have failed to fully identify the suspect vehicle. It is the utilization of an ALPR database in conjunction with other technologies produces an actionable investigative lead. For ALPR detections to be used to their fullest potential, that data must be connected to other relevant data sets.

The ultimate goal of connected data should be to allow for insights that are impossible to see currently or take too much time to consider. Departments should own all their data, including ALPR detections, and be able to link, connect, or integrate data sets as department leadership deems appropriate. When developing an ALPR program, agencies should ensure their vendors are aligned with this perspective and are capable of facilitating integrations with other law enforcement technology.

Beyond ALPR: AI-Enhanced Vehicle Detection

With advances in image processing technology, specifically those afforded by artificial intelligence and machine learning, it is becoming increasingly possible to identify a vehicle solely from an image. Artificial intelligence is able to focus on characteristics of a vehicle such as make, model, color, or distinguishing attributes/markings. These advanced image processing technologies improve the accuracy of ALPR systems and allow law enforcement to corroborate ALPR information. For example, they could assist with confirming that the vehicle associated with a detection matches the description in the registration record. Image-based detection and identification will continue to advance and improve the efficacy of ALPR technology.

Case Law Related to ALPR

License plates are required in every state to display proof of registration. Registration identifies a particular vehicle and confirms that it meets minimum state-mandated safety requirements to be operated on public roadways. In addition, operators of vehicles must be licensed to drive legally on public roads.

It is possible in many states to own a vehicle and, if it is never parked or operated on a public roadway, not be required to display license plates. Furthermore, one can own a car but have no authority to operate it, just as one can be licensed to drive a car but never actually own one. Collecting information related to people and vehicles are separate and distinct concepts, although not entirely mutually exclusive. The alpha-numeric characters of a license plate alone do not indicate who owns the vehicle or is licensed to operate it.

For more than 50 years, the United States Supreme Court, and many lower courts, have repeatedly acknowledged that vehicles are inherently subject to greater regulation when operated on public roadways. In the age of enhanced technology, ALPR invokes specific legal considerations:

- Reasonable privacy expectations of those in vehicles on public roadways
- Persistent tracking and the nature of ALPR technology
- The nexus between license plates and personally identifiable information
- Collecting and sharing ALPR data
- The degree of intrusion authorized by an ALPR hotplate detection

An examination of existing case law related to these concepts follows. There is often no bright-line precedent when considering emergent technology. In such instances, reasonable legal conclusions can be inferred from cases related to other technology and privacy issues already adjudicated by the courts.

Privacy Expectations on Public Roadways

In 1967, the U.S. Supreme Court clarified in *Katz v. U.S. (1967)* that "the Fourth Amendment protects people, not places." [9] The Fourth Amendment of the United States Constitution ensures:

> *[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.*

In *Cady v. Dombrowski (1973),* the U.S. Supreme Court noted that vehicles, while "effects," are constitutionally different from a person's home. The case also referenced the regularity with which police engage in activity unrelated to the enforcement of laws, such as maintaining the efficiency of the flow of traffic and ensuring the safety of those using the roadways. The Court acknowledged that this regular contact with automobiles contributes to police being more often in "plain view" of evidence, instrumentalities of a crime, or contraband.[10]

Delaware v. Prouse (1979) offers historic guidance concerning the constitutionality of stopping or seizing vehicles. The U.S. Supreme Court cites, "the permissibility of a particular law enforcement practice is judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests."[11] One can reasonably infer that photographing a plainly visible license plate, on a public roadway, or from a location plainly visible from a lawfully authorized location, with no intrusion upon the vehicle occupants or otherwise interfering with their movement or affecting any person's possessory interest in the vehicle or license plate, is not a seizure constitutionally.

Lower courts have routinely ruled that law enforcement officers may, without specific suspicion, check the status of a license plate against a law enforcement database.[12][13] Therefore, searching aggregated photographs, which contain no specific information about a particular vehicle owner or operator, even when correlated with additional information such as the time, date, and location of the photograph, does not constitute a search.

9 Katz v. United States, 389 United States Supreme Court. 347, (1967). https://supreme.justia.com/cases/federal/us/389/347

10 Cady v. Dombrowski, 413 United States Supreme Court. 433 (1973). https://supreme.justia.com/cases/federal/us/413/433

11 Delaware v. Prouse, 440 United States Supreme Court. 648 (1979). https://supreme.justia.com/cases/federal/us/413/433

12 Jones v. Town of Woodworth, Court of Appeal of Louisiana. 15-568. (2015). https://caselaw.findlaw.com/la-court-of-appeal/1717448.html

13 State v. Davis, 237 Or. App. 351, 239 P.3d 1002, Oregon Court of Appeals. (2010). https://caselaw.findlaw.com/la-court-of-appeal/1717448.html

Is ALPR Persistent Tracking?

The notion that vehicle travel on public roadways is an unavoidable element of modern living merits consideration, given how ALPR is deployed. Recent U.S. Supreme Court rulings related to law enforcement's use of other technologies have considered the inescapable and automatic nature of data collection. An analysis of these rulings is offered to differentiate the substantially greater capabilities of such technologies compared to those of ALPR.

Two recent U.S. Supreme Court rulings merit particular consideration for the use of technology to investigate the historical movement of persons. In *U.S. v. Jones (2012)*, the U.S Supreme Court held that police need a search warrant to install a covert GPS tracking device on a vehicle to monitor its location for an extended period of time. In *Carpenter v. U.S. (2018),* The Court ruled that police must secure a warrant before obtaining cell-site location information from service providers regarding an individual's location history.

The theme of both cases concerns the capacity that modern technology affords the government to explore comprehensive, specifically personal location information, which was not possible until the advent of recent ubiquitous technology. GPS and cell-site location information enable persistent automated tracking of a targeted individual's activity with such detail and scope that the techniques constitute a search. In the case of *Carpenter v. U.S. (2018),* the Government obtained 12,898 location points cataloging Carpenter's movements. This extensive amount of information amounted to an average of 101 data points per day during the period they obtained historical records.[14]

An ALPR system cannot independently predict life patterns accurately or be used to conduct real-time surveillance of any person or vehicle. Even if police acted with willful disregard for the protections of the Fourth Amendment, it is impossible to accomplish such a degree of ongoing surveillance using ALPR technology. A fixed ALPR camera may be able to collect information about every car that passes its location. Still, the data is limited to an otherwise anonymous characteristic of the vehicle, not automatically attributable to any individual without accessing other restricted databases, and for only a single moment in time at a single location.

Images of plates stored in the ALPR database are retained and made available for specified queries. Tangential information may include the nature of a vehicle's location, direction of travel, and any criminal justice information associated with the detection. As to the question of whether a collection of images from multiple cameras, aggregated in a searchable database implicates Fourth Amendment considerations, the US Supreme Court has not taken up precisely to what extent ALPR coverage, or how robust an ALPR database is, may trigger specific Fourth Amendment implications.

In *Commonwealth v. McCarthy (2020)*, the Massachusetts Supreme Judicial Court concluded that "While the defendant has a constitutionally protected expectation of privacy in the whole of his public movements, an interest which potentially could be implicated by the widespread use of ALPRs, that interest was not invaded by the limited extent and use of ALPR data in this case." The case involved law enforcement's use of four ALPR devices on two bridges to investigate a defendant's movements during a period of two months. In that case, the court ruled that the limited use of ALPR data did not violate the defendant's reasonable expectation of privacy.[15]

License Plates & Personally Identifiable Information (PII)

Individuals (people) are licensed, but a vehicle is registered. A vehicle is registered with an organization (typically a state), which then authorizes the vehicle to be driven on public roads and highways by a licensed driver. For example, passenger and commercial vehicles must be registered as a condition of use on a public thoroughfare. Upon registration, the state department of motor vehicles then issues a license plate which must be attached to the vehicle and openly displayed for vehicle identification purposes. The purpose of a license plate is to identify a vehicle uniquely, and it does not include personally identifiable information of any individual. By itself, a license plate number is an anonymous code unless combined with other registration information containing owner/operator information (i.e., a department of motor vehicles database or an employee or homeowner registration). Thus, an ALPR record is generated from publicly available data and corresponds with detecting a vehicle, not an individual, at a specific location and time.

The federal *Driver's Privacy Protection Act (DPPA)* was enacted in 1994 to "protect the personal privacy and safety

14 Carpenter v. United States, United States Supreme Court. 585 (2018). https://supreme.justia.com/cases/federal/us/585/16-402

15 Commonwealth v. McCarthy, 484 Massachusetts Supreme Judicial Court (2020). https://cases.justia.com/massachusetts/supreme-court/2020-sjc-12750.pdf

2784

of licensed drivers consistent with the legitimate needs of business and government." DPPA made it "unlawful" to access, disseminate, or otherwise misuse information held by a state's motor vehicle office, including information related to both drivers and vehicles, without the owner's consent or for another legitimate, legally authorized purpose, such as criminal justice purposes. ALPR systems do not automatically link to data governed by DPPA. Law enforcement can only obtain such protected information from other secure, access-restricted criminal justice databases.

The case of *Harrison Neal v. Fairfax County Police (2020)* examined the use of an ALPR system to passively scan and retain license plates that were not on a hotlist to determine if such a practice violated the state's *Government Data Collection and Dissemination Practices Act.*

A key element of the case was whether an ALPR system constitutes an information system governed by the Code of Virginia. The court found that the ALPR system did not, noting that the ALPR database can be searched only by license plate number, not by any person's information. Furthermore, the system does not gather identifying information about the vehicle owner. To acquire such personal data, an officer must query a wholly separate criminal justice database via a different computer program.[16]

California Code 1798.29 specifically expands the meaning of "personal information" to include information or data collected through the use or operation of an ALPR system. While not adjudicated by any court, ALPR information is considered personal information in California due to unique state legislation.

Data Collection & Sharing

A license plate is a required government instrument specifically intended to identify the vehicle to which it is affixed publicly. In the case of *United States v. Ellison (2006)*, the Court noted:

> *This court has yet to address in a published opinion the question of whether an individual has a reasonable expectation of privacy regarding their license plate. In two unpublished decisions, however, this court has agreed with the other circuits that have decided this issue by holding that no such privacy interest exists. The reasoning of these opinions, as well as that of the Supreme Court in related cases, leads us to agree that a motorist has no reasonable expectation of privacy in the information contained on his license plate under the Fourth Amendment.[17]*

Publicly viewing or photographing a displayed license plate constitutes activity protected by the First Amendment of the United States. The cataloging and subsequent sharing of such data remain largely regulated by state or local legislation. In the case of *U.S. v. Yang (2020),* the Ninth Circuit ruled that the defendant did not have standing to challenge government queries of a vendor's ALPR database for records of his movement when he kept a rental car beyond the contract due date. The court noted that Yang failed to establish that he had a reasonable expectation of privacy in the historical location information of the vehicle that was the subject of the query. The Court declined to address any potential privacy interests related to the warrantless use of ALPR technology.[18]

16 Harrison Neal v. Fairfax County Police, Record No. 191127, Supreme Court of Virginia (2020). https://cases.justia.com/virginia/supreme-court/2020-191127.pdf

17 United States v. Ellison, 462 F.3d 557, 561, United States Supreme Court. (6th Cir. 2006). https://caselaw.findlaw.com/la-court-of-appeal/1717448.html

18 United States v. Yang, No. 18-10341, United States Court of Appeals for the 9th Circuit (2020) https://law.justia.com/cases/federal/appellate-courts/ca9/18-10341/18-10341-2020-05-04.html

2785

ALPR Hits & Degrees of Intrusion

Several cases have affirmed that an ALPR hotplate detection, also referred to as a "hit," constitutes sufficient reasonable suspicion to affect a traffic stop. For example, in the case of *Hernandez-Lopez v. State (2013)*, the Georgia Court of Appeals held that an ALPR system merely aided the officer by augmenting his sensory faculties and that based on the alert provided by the ALPR, the officer had reasonable, articulable suspicion to conduct a traffic stop. [19]

Similarly, in the case of *Traft v. Commonwealth (2018)*, the Supreme Court of Kentucky held that an officer obtaining information linked to his license plate did not violate the defendant's rights under the Fourth Amendment. This information indicated that Traft had an outstanding bench warrant and, therefore, reasonable suspicion existed to stop the vehicle. Furthermore, the court noted that the license plate "was displayed in a place where he had no reasonable expectation of privacy."[20]

In the case of *Green v. City and County of San Francisco (2014)*, an ALPR system returned a hit based on a misread. The officer was transporting a prisoner at the time and could not verify the hit's validity. The image on the ALPR was "dark and blurry." The officer subsequently provided a description of the vehicle via police radio, including the incorrect license plate indicated by the ALPR system, not the actual plate displayed on the car. Dispatch ran the plate as provided and noted that it belonged on a pick-up truck.[21]

A second officer observed Green's sedan bearing the plate as broadcast by the first officer. However, this officer also failed to confirm whether the radioed license plate number matched the plates on Green's car. Consequently, Green was stopped, challenged at gunpoint by multiple officers, placed on the ground, and handcuffed. Green filed suit against the defendants, alleging claims under 42 U.S.C. 1983 and California state law for wrongful detention, false arrest, and excessive force. The Ninth Circuit ruled that "an unconfirmed hit on the ALPR does not, alone, form the reasonable suspicion necessary to support an investigatory detention."

While legally permissible to affect a stop based on an ALPR hit, independent verification of the validity of an ALPR alert should be considered a best practice. Verifying that the actual vehicle license plate and the read on the ALPR screen are safeguards against a potential unjustified intrusion upon any person. Such guidance should neither cause officers to hesitate when officer safety is a concern nor preclude officers from acting on indicators amounting to reasonable suspicion based on other observations coupled with their training and experience. However, inappropriate outcomes resulting from the use of law enforcement technology can have substantial repercussions on perceptions of police legitimacy and the continued availability of such tools.

In conclusion, ALPR systems detect license plates in public locations collecting information that is generally not considered private. Critical elements of an ALPR system, such as the extent of camera coverage, reasons for selecting fixed deployment locations, length of time that data is retained, and the extent to which the information is shared, may factor in with respect to if an ALPR system implicates Fourth Amendment considerations. The consistently responsible use and thoughtful deployment of ALPR technology will ensure that all civil rights and liberties are respected.

19 Hernandez-Lopez v. State, 319 Ga. App. 662, 738 S.E.2d 116, Court of Appeals of Georgia (2013) https://cite.case.law/ga-app/319/662

20 Traft v. Commonwealth, 539 S.W.3d 647 Supreme Court of Kentucky (2018) https://cite.case.law/ga-app/319/662

21 Green v. City and County of San Francisco, No. 11-17892, United States Court of Appeals for the 9th Circuit (2014). https://law.justia.com/cases/federal/appellate-courts/ca9/18-10341/18-10341-2020-05-04.html

2786

Conclusion

As stated in the introduction, this product contains suggestions and recommendations, which, if adopted, will maximize ALPR technology's effectiveness while ensuring it is used ethically and responsibly. While this product provides a robust evaluation of the technology, it is impossible to cover every aspect of the technology. Therefore, the Working Group recommends that law enforcement use the tenets discussed in this document to help evaluate decisions regarding the use of ALPR technology. This must include the potential impact of ALPR technology on public trust and the community served. It is essential that, when implementing any technology program, law enforcement operate in a manner that is thoughtful, disciplined, and contextually mindful of its constituencies.

For those agencies wishing to implement an ALPR program but are still determining how to move forward, collaboration with other entities who have already developed robust, responsible programs is recommended. The sharing of best practices in crime-fighting technology among law enforcement has a history of beneficial impacts. Law enforcement must be good stewards of information and policies and be willing to share this with fellow law enforcement agencies wishing to begin using ALPR.

Law enforcement's use of ALPR is ubiquitous because the information these systems provide is advantageous. ALPR data has aided in countless successful criminal investigations and has proven to be one of the most valuable technologies available to law enforcement. Few technologies have aided law enforcement in keeping communities safe like ALPR. However, the capabilities of ALPR technology are continuously evolving, and the MCCA will continue to monitor it. The MCCA will remain engaged with all interested stakeholders and communicate the latest information with member agencies and the entire law enforcement profession so best practices can be adjusted as needed.

Acknowledgments

Major Cities Chiefs Association would like to extend a special thanks to the ALPR Working Group and its members listed below. The contents of this document would not be possible without the collaboration between these law enforcement professionals and the technology vendor participants.

Kelly Bluth
DETECTIVE
Las Vegas Metropolitan Police Department

Blake Bullock
SENIOR DIRECTOR & GM FLEET PRODUCTS
Axon

Paige Burley
CLIENT FACING DEPLOYMENT
Peregrine

Gabriel Candelaria
LIEUTENANT
Dallas Police Department

Jeffrey Carroll
ASSISTANT CHIEF OF POLICE
Metropolitan Police Department Washington D.C.

Laura Cooper
EXECUTIVE DIRECTOR
Major Cities Chiefs Association

Travis Eicher
LMPD TECHNICAL SERVICES
Louisville Police Department

Dan Gillespie
TECHNOLOGY PROGRAM MANAGER
Louisville Police Department

Jeremy Harrison
MAJOR
Oklahoma City Police Department

Kyle Hoertsch
PRODUCT DEVELOPMENT MGR ENTERPRISE SOLUTIONS
Motorola Solutions

Milton Wyatt Martin
ASSISTANT CHIEF
Houston Police Department

Matt Melton
SENIOR BUSINESS DEVELOPMENT MANAGER
Amazon Web Services

Jason Olin
DIRECTOR OF GOVERNMENT AFFAIRS
Major Cities Chiefs Association

Samuel Paul
DEPUTY
Los Angeles Sheriff's Department

Christian Quinn
MANAGING PRINCIPAL
Fulcrum Innovation LLC

Jeremy Slavish
SENIOR BUSINESS DEVELOPMENT MANAGER
Amazon Web Services

Paul Steinberg
SENIOR VICE PRESIDENT OF TECHNOLOGY
Motorola Solutions

Josh Thomas
VP OF POLICY AND COMMUNICATIONS
Flock Safety

Matthew Thomas
COMMANDER
Indianapolis Metropolitan Police Department

Mark Torres
COMMANDER - REAL TIME CRIME CENTER
Albuquerque Police Department

Mike Wagers
SENIOR VICE PRESIDENT STRATEGIC INITIATIVES
Axon

Dalton Webb
DIRECTOR OF RTCC STRATEGY
Flock Safety

Paden Weber
INTELLIGENCE OFFICER
Las Vegas Metropolitan Police Department

William Zelms
CAPTAIN
Virginia Beach Police Department

GRAPHIC DESIGN BY PADEN WEBER

2788

Definitions

Automated License Plate Reader/Recognition (ALPR): ALPR systems comprise cameras that capture an image of a vehicle's license plate and use Optical Character Recognition (OCR) to automatically read license plate characters.

Contextual Photo/Image: An overview image of the area around a detection.

ALPR Record/Detection: Is generated when an instance of a vehicle license plate is detected, imaged, and processed to identify the plate.

Hit: A detection of a license plate that matches a plate previously registered on a hotlist or hotplate.

Hotlist: A file that contains the license plate numbers of stolen vehicles; AMBER, SILVER, or other law enforcement alerts; lists of license plate numbers known to be associated with specific individuals, such as wanted or missing individuals.

Hotplate: A license plate with a wanted status. It may also be entered into a system designed to provide a notification of future detections.

Misread: An incorrect translation of a license plate.

Fixed Camera: An ALPR camera that is affixed to a non-moving structure.

Mobile Camera: A vehicle-mounted camera.

Law Enforcement Data: ALPR data collected by law enforcement-owned ALPR cameras.

Data Retention: Refers to the amount of time that the collected data will be preserved.

Personally Identifiable Information (PII): Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.[1]

National Crime Information Center (NCIC): An electronic clearinghouse of crime data, such as mug shots and crime records, available to virtually every criminal justice agency nationwide.[2]

1 Guidance on the Protection of Personally Identifiable Information, U.S. Department of Labor. https://www.dol.gov/general/ppiihttps://www.dol.gov/general/ppii

2 National Crime Information Center (NCIC), Federal Bureau of Investigation. https://le.fbi.gov/informational-tools/ncic

2789

Appendix A – Success Stories

Homicide

After committing a homicide, the suspect fled the scene by vehicle. During the investigation, investigators learned that the suspect drove a specific vehicle with damage to the body. Using the ALPR system, detectives created a geographic boundary around the crime location. While reviewing the historical ALPR detections from that immediate area, a vehicle matching the suspect's vehicle description was identified. Detectives then discovered the actual license plate registration information, which returned to the primary suspect. Another query of that vehicle through the ALPR system revealed that the suspect vehicle had fled the jurisdiction immediately after the homicide occurred. This was later confirmed and corroborated by the suspect's cell phone location records.

Homicide

During a road rage incident resulting in a shooting and murder, the suspect was reportedly driving a black hearse. Responding officers obtained the victim's license plate number and checked it through the ALPR system. The officers located an ALPR record of the victim's vehicle passing an ALPR deployment site three minutes before the shooting. The officers checked for other vehicles driving past the ALPR cameras around the same time as the victim. The vehicle driving directly behind the victim was a black hearse. The ALPR data, along with a tip from the public, were pivotal in the arrest. The suspect gave a full confession. The arrest occurred within only a few hours of the crime.

Homicide

The victim knocked on the suspect's hotel room door. Annoyed by the knocking, the suspect opened the door and immediately shot and killed the victim. Surveillance footage of the suspect and his associate leaving captured the type of vehicle used by the suspect but did not capture the license plate. An ALPR camera system was stationed just down the street from the hotel. Officers reviewed the ALPR database for the time frame around the homicide. One minute before the 911 call, the ALPR camera captured a detection of a vehicle matching the one observed in the hotel surveillance. Armed with the vehicle registration information, the vehicle's lien holder was contacted, which provided new investigative leads. Within 11 hours of the shooting, officers located the suspect's vehicle hidden in a home's garage. The suspect and his associate were detained, provided a confession, and later charged with homicide.

Burglary

A police agency used ALPR to identify two suspect vehicles involved in a burglary. Multiple suspects in two vehicles committed a residential burglary, with the resident shooting and killing one of the suspects. Doorbell camera videos were recovered, and homicide detectives used them to establish a timeline. ALPR searches focused on the timeline, which resulted in ALPR scans for both suspect vehicles. A subject associated with one of the vehicles was later determined to be involved and arrested for burglary.

Sexual Assault and Attempted Murder

A victim met the suspect at a bar. They left and the suspect drove them to the desert, where he sexually assaulted, beat, strangled, and ran her over. The vehicle plate from the bar where the incident began was queried in the ALPR system. Historical detections placed the suspect vehicle in the desert where the victim was assaulted and left behind, along with other areas where the victim reported they had driven before the assault. The ALPR data was critical in the arrest of this violent attacker.

Fatal Hit-and-Run Traffic Accident

ALPR was used to identify the suspect vehicle that left the scene of a fatal traffic accident after hitting two people. The make and model of the vehicle were identified but not the license plate. The license plate and other supporting evidence were discovered by leveraging the ALPR system. After the crime occurred, ALPR detection records showed significant damage to the suspect vehicle.

2790

Kidnapping

A male subject attempted to grab a female in a business parking lot. Video surveillance captured the subject and his vehicle. Detectives used video footage to determine the suspect vehicle's make, model, and year range. A query of the ALPR system provided sufficient information to confirm the suspect vehicle and registration. The male was later identified. A records check revealed he had two prior arrests for sexual assaults. He was later located and arrested for the crime of kidnapping.

Arson

A subject set fire to the sign and lawn outside an FBI office building. Surveillance footage showed a gold Chevy Tahoe with distinctive damage to the passenger and rear sides of the vehicle. The license plate number was not visible. Analysts searched more than 6,000 images in the ALPR database, looking for Chevrolet SUVs similar to the one in the surveillance footage. After searching the ALPR database, analysts found a vehicle with matching damage, identified the registered owner, then disseminated a bulletin for officers to locate the vehicle. Initially, officers could not locate the registered owner, who was transient. A few days later, a patrol officer spotted the vehicle based on the bulletin and detained the suspect. The suspect was positively identified and linked to the original arson and another one in a different part of the state. Less than one month later, the suspect accepted the criminal prosecution agreement offered by the prosecutors.

2791

Appendix B – Myths and Misconceptions

A review of case law provides a snapshot of the legalities supporting the use of ALPR technology. In contrast, some misinformation exists on the use of ALPR technology by law enforcement. Therefore, reviewing and understanding the myths and misconceptions about ALPR in law enforcement is essential.

MYTH

ALPR detections contain private, personally identifying information.

REALITY

ALPRs are designed to capture three details when a vehicle passes through their view: a photograph of the vehicle, the characters on the license plate of the vehicle, and the location, date, and time when the vehicle passes the ALPR.

Publicly-owned ALPR systems read the license plates of vehicles on public roadways and capture information that is generally not considered private. For example, if an individual were to stand by the side of a public road and take a picture of every vehicle that passed them, write down its plate number, and record the date and time, they would be within their legal rights to do so. Likewise, a person could place a camera on their property facing a public throughway and capture the same information an ALPR does. In *U.S. v. Ellison (2006)*, the Court explained that not only is there no privacy interest in a license plate number, but a subsequent entry into a computer system to retrieve other non-private information does not constitute a search.[3] By states mandating each vehicle operating on the roadway publicly display a license plate and even illuminate it at night, the expectation is for the license plate to be read at any time while on a public roadway.

An ALPR system does not automatically capture or record restricted information contained in an individual's motor vehicle records, such as their name, address, phone number, Social Security Number, driver identification number, etc. *The Driver's Privacy Protection Act of 1994* requires all states to protect this personal information ensuring ALPR reads are anonymous until additional steps are taken to access separate statutorily regulated databases. Therefore, when a law enforcement officer needs to access motor vehicle records based on data captured by an ALPR, they would need to perform the same manual processes to retrieve this information as they would in other investigative circumstances. Additionally, adequate policies limit access to ALPR data by requiring justification for the review of individual ALPR records. This effectively ensures that most ALPR-captured data is never even accessed before it is purged.

Therefore, retrieving non-public information based on ALPR data requires law enforcement to adhere not only to the policies and laws regarding the ALPR data but also to the policies and laws for accessing the restricted databases housing driver's license and vehicle information. In summary, ALPR systems do not grant expanded access to any non-public records databases, nor do they circumvent the auditing processes that are in place to ensure restricted data is accessed only for official use and as permitted by law.

3 United States v. Ellison, 462 F.3d 557, 561, United States Supreme Court. (6th Cir. 2006). https://caselaw.findlaw.com/la-court-of-appeal/1717448.html

MYTH

ALPR technology is a form of mass surveillance.

REALITY

Guided by proper policy and processes, ALPRs are effective tools for law enforcement to narrow the focus of investigations and limit negative collateral impacts when policing high-crime areas.

A scenario most major city police departments are familiar with is as follows: A motorist is stopped by police only to later be released and sent on their way in a case of mistaken vehicle identity. Their misfortune was caused by driving a vehicle matching the general description of one recently broadcasted of a suspect vehicle in a violent crime. Though the detention is usually short-lived, the trauma it causes may not be. This type of "wrong place, wrong time" scenario is most likely to occur when non-specific or incorrect information is relayed to officers during an in-progress incident. Even a single negative experience like this can spread quickly throughout a community, jeopardizing efforts to build trust. Unfortunately, these scenarios most commonly affect residents in neighborhoods disproportionately impacted by violent crime and gun violence. The use of ALPRs can help mitigate these occurrences.

ALPRs provide an additional mechanism to corroborate or refute witness accounts of suspect vehicles. This helps narrow the focus of law enforcement when canvassing and provides officers with the increased ability to bypass lookalike vehicles and only interact with the cars that truly contain the distinct characteristics of the vehicle suspected in the crime.

A common talking point designed to instill fear in ALPRs technology is that they "could" be used to track people involved in first amendment protected activities. The purpose of robust agency policy is to restrict use to legally permissible actions and ensure accountability if rules are broken. It must be noted that the same policies and laws governing law enforcement's actions without technology still apply when using technology. In fact, the audit trails in technology ensure that a hindsight review of any actions taken is afforded an even more detailed perspective than the actions taken without records produced by technology.

2793

Appendix C – State-Level Laws and Regulations

At least 16 states have statutes regarding the use of ALPR or the retention of data collected by ALPR technology. This information was derived from a database maintained by the National Conference of State Legislatures.[4] The states and their laws are as follows:

Arkansas-Ark. Code §§ 12-12-1801 to 12-12-1808

Prohibits use of ALPRs by individuals, partnerships, companies, associations or state agencies. Provides exceptions for limited use by law enforcement, by parking enforcement entities or for controlling access to secure areas. Prohibits data from being preserved for more than 150 days.

California-Calif. Veh. Code § 2413

Provides that the California Highway Patrol (CHP) may retain data from a license plate reader for no more than 60 days, unless the data is being used as evidence in felony cases. Prohibits selling or making available ALPR data to non-law enforcement officers or agencies. Requires CHP to report to the legislature how ALPR data is being used.

California-Calif. Civil Code §§ 1798.29, 1798.90.5

Establishes regulations on the privacy and usage of automatic license plate recognition (ALPR) data and expands the meaning of "personal information" to include information or data collected through the use or operation of an ALPR system. Imposes privacy protection requirements on entities that use ALPR information, as defined; prohibit public agencies from selling or sharing ALPR information, except to another public agency, as specified; and require operators of ALPR systems to use that information only for authorized purposes.

Colorado-Colo. Rev. Stat. § 24-72-113

Requires that video or still images obtained by passive surveillance by governmental entities, such as images from monitoring cameras, must be destroyed within three years after the recording of the images. Specifies that the custodian of a passive surveillance record may only access the record beyond the first anniversary after the date of creation of the record if there has been a notice of claim filed, or an accident or other specific incident that may cause the passive surveillance record to become evidence in any civil, labor, administrative, or felony criminal proceeding. Creates exceptions allowing retention of passive surveillance records of any correctional facility, local jail, or private contract prison and passive surveillance records made or maintained as required under federal law.

Florida-Fla. Stat. § 316.0777

Creates a public records exemption for certain images and data obtained through the use of an automated license plate recognition system and personal identifying information of an individual in data generated from such images. Provides that images and data containing personal information obtained from automated license plate recognition systems are confidential. Allows for disclosure to criminal justice agencies and to individuals to whom the license plate is registered in certain circumstances.

Georgia-Ga. Code § 35-1-22

License plate data may be collected and accessed only for a law enforcement purpose. The data must be destroyed no later than 30 months after it was originally collected unless the data are the subject matter of a toll violation or for a law enforcement purpose. Allows sharing of captured license plate data among law enforcement agencies. Law enforcement agencies deploying an automated license plate recognition system must maintain policies for the use and operation of the system, including but not limited to policies for the training of law enforcement officers in the use of captured license plate data. License plate data collected by a law enforcement agency is not subject to public disclosure.

4 Automated License Plate Readers: State Statutes," National Conference of State Legislatures. https://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx

2794

Maine-29-A M.R.S.A. § 2117-A(2)

Prohibits the use of automatic license plate recognition systems except for certain public safety purposes. Provides that data collected is confidential and may be used only for law enforcement purposes. Data collected may not be stored more than 21 days.

Maryland-Md. Public Safety Code § 3-509

Specifies the procedures and protocols that a law enforcement agency must follow in connection with the operation of an "automatic license plate reader system" and "captured plate data." Requires the State Police to adopt procedures to address who has access to the data and training for those individuals and to create an audit process. Provides that data gathered by an automatic license plate reader system are not subject to disclosure under the Public Information Act.

Minnesota- Minn. Stat. §§ 13.82,13.824, 626.8472

Relates to data practices; classifies data and provides procedures related to automated license plate readers; provides the data that may be collected by such readers; relates to requirements for the sharing of such data among law enforcement agencies; requires the maintenance of a public log recording the uses of such data; requires related records maintenance and the auditing of such records; requires written procedures governing access to the data; requires certain notification when setting up readers.

Montana-Mont. Code Ann. §§ 46-5-117 to -119

Prohibits the use of license plate readers by an agency or employee of the state or any subdivision of the state on any public highway. Provides exceptions for specific agencies or purposes, such as state or local law enforcement, if specified requirements are met. Except as provided, license plate data captured by law enforcement may not be preserved for more than 90 days after the date that the data is captured.

Nebraska- Neb. Rev. Stat. § 60-3201 to 3209

Requires any governmental entity that uses an automatic license plate reader (ALPR) system to adopt a policy governing use of the system. Governmental entities also must adopt a privacy policy to ensure that captured plate data is not shared in violation of this act or any other law. The policies must be posted on the internet or at the entity's main office. Requires annual reports to the Nebraska Commission on Law Enforcement and Criminal Justice on ALPR practices and usage. Provides that captured plate data is not considered a public record.

New Hampshire-N.H. Rev. Stat. Ann. §§ 261.75-b, 236.130

Restricts the use of automated license plate readers to local, county and state law enforcement officers, who shall only use the devices subject to specified conditions and limitations and for specified purposes. Provides that records of number plates read shall not be recorded or transmitted anywhere and shall be purged from the system within 3 minutes of their capture, unless the number resulted in an arrest, a citation or protective custody or identified a vehicle that was the subject of a missing or wanted person broadcast.

North Carolina-N.C. Gen. Stat. §§ 20-183.30 to .32

Requires state or local law enforcement agencies to adopt a written policy governing the use of an ALPR system that addresses databases used to compare data obtained by the system, data retention and sharing of data with other law enforcement agencies, system operator training, supervision of system use, and data security and access. Requires audits and reports of system use and effectiveness. Limits retention of ALPR data to no more than 90 days, except in specified circumstances. Provides that data obtained by the system is confidential and not a public record.

2795

Oklahoma-Okla. Stat. §§ 47-4-606.1

Provides that participating law enforcement agencies may use automatic license plate reader systems to access and collect data for the investigation, detection, analysis or enforcement of the state's compulsory insurance law. States that data collected under the program may not be used by any individual or agency for purposes other than enforcement of the compulsory insurance law, prohibits sale of the data under the program, and provides that data is exempt from the Oklahoma Open Records Act, except when retained as evidence of a violation of the compulsory insurance law. These provisions do not prohibit the use of any other automated license plate reader system by an individual or private legal entity for lawful purposes.

Tennessee-Tenn. Code §§ 55-10-302, 10-7-504(a)

Provides that any captured automatic license plate data collected by a government entity may not be stored for more than 90 days unless they are part of an ongoing investigation, and in that case provides for data to be destroyed after the conclusion of the investigation. Captured plate data from automatic license plate reader systems must be treated as confidential and shall not be open for inspection by members of the public.

Utah-Utah Code §§ 41-6a-2001 to -2005

Provides that a governmental entity may not use an automatic license plate reader system except for specified uses, such as by law enforcement agencies for the purpose of protecting public safety or conducting criminal investigations and by other government entities for limited other purposes. Provides that captured plate data are a protected record under the Government Records Access and Management Act, if the captured plate data are maintained by a governmental entity. Provides that captured plate data may only be shared for specified purposes, may only be preserved for a certain time and may only be disclosed pursuant to specific circumstances such as a disclosure order or a warrant. Government entities may not use privately held captured plate data without a warrant or court order, unless the private provider retains captured plate data for 30 days or fewer. Allows an institution of higher education to use automatic license plate readers under certain circumstances.

Vermont- 23 V.S.A. §§ 1607, 1608

Requires a law enforcement officer to be certified in the use of an automated license plate reader to operate such a system. Provides that active system data may only be accessed by an officer with a legitimate law enforcement purpose for the data. A legitimate purpose includes a person's defense against certain charges and does not include enforcement of parking or traffic violations other than commercial motor vehicle violations. Limits retention and access to information gathered through the use of an ALPR system. Requires the Department of Public Safety to adopt rules to implement the law. Requires the Auditor of Accounts to examine requests for data to determine whether the request and the release complied with the law.

2796

Appendix D – CJIS Security Policy

Agencies that wish to use the CJIS Security Policy to assess the security practices of a service provider that will be handling ALPR data should consider the following sections:

- Private Contractor User Agreements and FBI-CJIS Security Addendum [5.1.5]: Private contractors who perform criminal justice functions for a Criminal Justice Agency (CJA) shall be permitted to access CJI pursuant to an agreement between the CJA and the contractor that incorporates the FBI-CJIS Security Addendum approved by the Director of the FBI.
- Agency User Agreements [5.1.1.6]: Fingerprint-based background checks and written agreement with the agency when required.
- Secondary Dissemination [5.1.3]: If data is released to another authorized agency and not part of a primary information exchange agreement, this shall be logged.
- Security Awareness Training [5.2]: All personnel with access to CJI (Criminal Justice Information) shall receive security awareness training within six months of assignment, and biennially thereafter.
- Security Training Records [5.2.3]: Records of security awareness training shall be kept current and maintained by a Security Officer (CSO).
- Reporting Structure and Responsibilities [5.3.1.1]: Establishment of a primary Point of Contact (POC) for CJIS incident handling and response.
- Events [5.4.1.1]: Description of the events that must be logged within the system.
- Audit Monitoring, Analysis and Reporting 5.4.3]: Responsibility for review and analysis of audit records, at a minimum of once a week, to look for inappropriate or unusual activity.
- Audit Record Retention [5.4.6]: The agency shall retain audit records for at least one year.
- Least Privilege [5.5.2.1]: The agency shall approve individual access privileges and enforce the most restrictive set of rights and privileges needed by users for the performance of specified tasks. Logs maintain access privilege changes for a minimum of one year or at least equal to the agency's record retention policy, whichever is greater.
- Access Control Mechanisms 5.5.2.4]: One or more of the following must be employed: access control lists (users, groups, machines), resource restrictions (permission sets), encryption and strong key management, application-level access control.
- Unsuccessful Login Attempts [5.5.3]: CJIS Security Policy requires that after five consecutive invalid attempts, the account shall be locked out for a minimum of 10 minutes.
- System Use Notification [5.5.4]: The system shall allow a notification message to be displayed to let users know a) they are accessing a restricted system, b) usage is monitored, recorded and subject to audit, c) unauthorized use is prohibited and may result in penalties, and d) use of the system indicated consent to monitoring.
- Session Lock [5.5.5]: CJIS Security Policy requires that the system shall prevent access via a session lock after a minimum of 30 minutes of inactivity.
- Remote Access [5.6]: Rules for monitoring and controlling remote access via the internet.
- Use of Originating Agency Identifiers in Transactions and Information Exchanges [5.6.1.1]: An FBI-issued ORI number shall be assigned at the agency level and attached to all activities by the agency's users.
- Password [5.6.2.1.1]: Requirements and standards for passwords.
- Personal Identification Numbers [5.6.2.1.2]: Best Practices on PIN use.
- Advanced Authentication [5.6.2.2]: Advanced Authentication requirements.
- Identifier Management [5.6.3]: Requirements of agencies to manage user identifiers.
- Network Diagram [5.7.1.2]: Requirements for a network topological diagram.

2797

- Media Protection [5.8]: Requirements for security and protection of electronic and physical media.
- Physical Protection [5.9]: Requirements for physical security and access controls around all hardware, software and media.
- System and Communication Protection and Information Integrity [5.10]: Prevent CJI from being transmitted unencrypted across the public network.
- Boundary Protection [5.10.1.1]: Ensure that failure of boundary protection mechanisms do not result in unauthorized release of information.
- Encryption [5.10.1.2]: Minimum of 128 bit encryption when CJI data is transmitted beyond the physical security boundary.
- Intrusion Detection Tools and Techniques [5.10.1.3]: Requirements for intrusion detection tools.
- Cloud Computing [5.10.1.5 and Appendix G.3]: Recommendations for use of cloud computing and assessment of cloud computing service providers.
- Partitioning and Virtualization [5.10.3]: Requirements for partitioning of data and virtualization of resources.
- Patch Management [5.10.4.1]: Requirements for management of software patches.
- Malicious Code Protection [5.10.4.2]: Virus Protection requirements.
- Spam and Spyware Protection [5.10.4.3]: Spam and Spyware Protection requirements.
- Security Alerts and Advisories [5.10.4.4]: Guidance for alerts and advisories.
- Personnel Security [5.12]: Fingerprint-based background checks and rules based on findings.
- Personnel Termination [5.12.2]: Terminated employees shall immediately have access revoked.
- Personnel Sanctions[5.12.3]: Process for employees failing to comply with security policies.
- Mobile Devices [5.13]: Where appropriate, the technology partner must support the agency's mobile device practices (patch management, etc.)

2798

Appendix E – ALPR Audit and Transparency Report Template

The following template provides a rudimentary example of the details and considerations in providing a published report about the performance and effectiveness of an ALPR program.

Automated License Plate Reader Program
Annual Transparency Report

Introduction

The introduction should provide context and background as to what the report is addressing. The introduction defines the specific objectives and purpose of the report. It indicates any problems that may exist and provides answers to problems explored. Finally, the introduction will preview the report and outline the report structure.

Discussion

This is the main body of the report, and it has two primary purposes. The first is to share and explain the conclusions. The second is to justify any recommendations that may be made in the report.

Specific data points that may be considered:

- Number of detections
- Number of hotplate hits
- Number of queries conducted by users
- Number of arrests directly related to ALPR
- Number of user-generated hotplates
- Breakdown of hotplate hit types
- Year-over-year analysis and trends

Conclusion

This section should relate to the information shared in the report. It should be specific to the objectives of the report. It may also address any issues that may be interpreted from the information shared. The conclusion should be brief, logical, and specific.

Recommendations

Recommendations shared should point to future action that can be completed. Recommendations should be feasible, action-oriented and arranged in order of importance.

Massachusetts Department of State Police
Automated License Plate Recognition (ALPR) System
Memorandum of Understanding and Agreement

THIS AGREEMENT, made and entered into this 01 day of June, 2022 by and between the Department of State Police, hereinafter referred to as "Department," and the

Taunton 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-1I 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	Chief Edward J. Walsh Taunton Police Department
	06/06/2022
Date	Date

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**TRF-11**
Subject:	
Automatic License Plate Recognition	

Policy

The availability and use of the Automatic License Plate Recognition (ALPR) System provides opportunities for enhancing the productivity and effectiveness of law enforcement agencies. The ALPR System also provides opportunities to increase public and officer safety.

The 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.

Purpose

To establish guidelines and procedures for the proper use and application of the ALPR System within the Department of State Police, and to provide guidelines and principles for the collection, access, use, dissemination, and retention of ALPR information by members 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.

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 through, utilization of the ALPR System.

ALPR Data Query Logs: A record of a search or query of ALPR data.

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.

Definitions and Acronyms, continued

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, Incapacitated or Endangered Persons, 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.

Authorized Uses

The provisions of this policy are provided to support authorized uses of ALPR information. Authorized uses may include, but are not limited to, the following:

- Investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime;
- Enhance Department's AMBER/SILVER or other law enforcement alerts and real-time response capability by deploying and networking ALPRs across the state to more rapidly identify and locate vehicles related to potential child-abduction or other serious crimes;
- Alert law enforcement that a particular license plate on a "hot list" (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 and assist in locating dangerous and wanted individuals;
- Identify plates associated with potential witnesses and/or victims of crime;
- Support the Department's homeland security mission by protecting critical infrastructure from subjects who intend to damage or disrupt the systems and locations that allow for travel and the free flow of commerce;

Authorized Uses, continued

- Identify vehicles linked to stolen license plates or other motor vehicle traffic violations;
- Provide situational awareness for law enforcement related to public safety or otherwise relevant to their authorized duties;
- Support local, state, federal, and tribal public safety departments in the identification of subjects associated with/as targets of criminal investigations;
- Support law enforcement response to critical incident responses and special events;
- Support special operations, such as high-crime-area patrols, gang investigation/suppression, operating under the influence initiatives, enforcement details, directed criminal investigations, and other investigations; and
- Support emergency and public safety situations including, but not limited to terrorist threats, kidnappings, missing persons, and felons actively traveling to or from a crime scene.

ALPR Administrator

The Division Commander of Field Services (DFS) shall:

- Designate a 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:

- Ensure the proper selection of personnel approved to operate the ALPR System and maintain an adequate number of trained and authorized users;
- Authorize any requests for ALPR System use or data access according to Department policy;
- Coordinate with all Divisions to ensure resources are available and deployed to meet Departmental investigative needs;
- Ensure 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;
- Designate users who have been properly trained in the use and operational protocols of the ALPR System;
- Allow access to the ALPR System for those users with an approved login and password; and
- Ensure that any changes in hardware, software, policy, or law are the subject of continuing in-service training or bulletins.

Subject: Automatic License Plate Recognition	Number: TRF-11

ALPR Procedures

The use of ALPR technology shall be approved by the Colonel/Superintendent or designee.

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 members of this Department or by other law enforcement agencies through the ALPR Administrator.

ALPR Operations

Members using the ALPR System shall:

- Ensure, at the start of each shift, 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.

ALPR Alerts/Hits

The member shall, prior to initiation of a stop based on an ALPR Hit or Alert:

- Visually verify that the vehicle plate number matches the plate number run by the ALPR System, including both:
  - Alphanumeric characters of the license plate; and
  - The state of issue.
- Verify the current status of the plate through:
  - The Commonwealth's Criminal Justice Information System (CJIS), or
  - National Crime Information Center (NCIC), or
  - Department's Records Management System (RMS), or
  - Another appropriate source of data, as soon as practicable.

ALPR Alerts/Hits, continued

License plate numbers and date/time location collected through an ALPR, when taken alone, may not be sufficient to identify the individual associated with the vehicle. The Department may be able to link the ALPR information to an individual through, or in combination with, additional information from other sources, such as a check of vehicle registration. It is thus the investigative process that ultimately identifies individuals and not solely a reliance on the information obtained from the ALPR system's automated collection of license plate numbers.

Manual Entry of Data/Manual Hot List

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);
- Investigative needs;
- 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 one (1) year or less.

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.

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;

ALPR Data: Logs, Sharing, Dissemination, and Retention, continued

- 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 and/or intimidating any individual or group;
- Targeting of any individual or group by means of camera placement or data use in a discriminatory manner; and
- Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

The Department protects all ALPR information as personally identifiable information (PII) beeause ALPR information may be combined with other information to specifically identify a unique individual (i.e., the identity of an individual could be directly or indirectly inferred by using information that is linked or linkable to that individual).

Information 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 point of contact, in writing or electronically, when the Department's ALPR information is alleged, suspected, or found to be erroneous or deficient.

Security

The following shall apply to ALPR system and information security:

- The Department of Criminal Justice Information Services of the Executive Office of Public Safety and Security will operate ALPR servers in a secure facility protected from external intrusion and will utilize secure internal and external safeguards against network intrusions. Any access to DCJIS ALPR information from outside the facility will be allowed only over secure networks;
- The Department and DCJIS will store ALPR information in a manner that ensures that it cannot be added to, modified, accessed, or purged except by personnel authorized to take such actions;
- Access to Department ALPR information will be granted only to personnel whose positions and job duties require such access and who have successfully completed a background check and training;
- Usernames and passwords to ALPR information are not transferrable, must not be shared by Department personnel, and must be kept confidential;
- Queries made to the Department's ALPR information will be logged into the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit; and
- The Department and DCJIS will maintain an audit trail of accessed, requested, or disseminated Department-held ALPR information. The audit trail will be retained for a minimum of one year. It will include all requests for access to ALPR information, the specific purposes for each request, and what ALPR information was disseminated to each individual in response to that request.

State Central Repository

The Department has agreed to:

- Electronically submit captured ALPR data to the state repository maintained by the DCJIS at the Commonwealth's Public Safety Data Center.

The Department and its users agree to the terms of this policy and to the Commonwealth of Massachusetts *Global Justice and Public Safety Information Sharing Policy* of the DCJIS.

Policy Review

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.

Because existing technology may progress and new technology may develop, giving rise to both legal and technological issues, the Department will monitor and assess the appropriateness of this policy, and make amendments as necessary.

Subject:	Number:
Automatic License Plate Recognition	**TRF-11**

References: Executive Office of Public Safety and Security (EOPSS) – The Commonwealth of Massachusetts Global Justice and Public Safety Information Sharing Policy;
EOPSS – Department of Criminal Justice Information Services – Automatic License Plate Recognition System Central Repository Companion Policy;
MPAC: 41.3.9.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

MOTOROLA SOLUTIONS

ORIGINAL INVOICE

Motorola Solutions, Inc.
500 West Monroe
Chicago IL 60661
United States
Federal Tax ID: 36-1115800

Transaction Number	Transaction Date	Transaction Total
8281711482	10-SEP-2023	**188,164.80 USD**

P.O. Number	P.O. Date	Customer Account No
2024MOTRLU07POL20232	14-AUG-2023	1011906651

Payment Terms	Payment Due Date
Net Due in 30 Days	10-OCT-2023

Visit our website at www.motorolasolutions.com

Bill To Address

MASSACHUSETTS STATE POLICE
ATTN: Accounts Payable
470 WORCESTER RD
FRAMINGHAM MA 01702
United States

Invoice Receipt date 9-11-23

"The equipment, goods or services for which this payment is made were received on_____

certified by_____

signature date_____

Ship To Address

MHQ MUNICIPAL SUPPLY
401 ELM ST
MARLBOROUGH MA 01752
United States

IMPORTANT INFORMATION

Ultimate Destination
United States

Freight
PREPA

Inco Te

MARLBOROUGH,MA,US,INCO
TERMS® 2010

For all invoice payment inquiries contact
AccountsReceivable@motorolasolutions.com
Telephone: 800-247-2346
Fax: +1(631)883-4238

Sales Order(s): 3203078421
Delivery Number(s): 9109994447

SPECIAL INSTRUCTIONS / COMMENTS

Line Item #	Item Number	Description	Qty.	Unit Price (USD)	Amount (USD)
1	4RE-WRL-KIT-103	CONFIGWIRLESKIT MTIK802.11AC,POE,5GHZANT **SO Line #:** 1.1 **Ship Date:** 09-SEP-2023	24	250.00	6,000.00
2	BRK-ANT-NMO-001	CBL, WIFI VHCL ANT MNT, NMO, 17'L **SO Line #:** 2.1 **Ship Date:** 09-SEP-2023	24	60.00	1,440.00
3	WGP02225-130-KIT2	BRKT4RE DISP/VISTA/CAMVR POST 2020+EXPL **SO Line #:** 4.1 **Ship Date:** 09-SEP-2023	24	0.00	0.00
4	WGB-0708A	M500 ICV SYSTEM W/RCAM V300 WIFI DCK,SPS SO Line #: 7.1 Ship Date: 09-SEP-2023	24	6,315.00	151,560.00

Please detach here and return the bottom portion with your payment

Payment Coupon

Transaction Number	Customer Account No	Payment Due Date	Transaction Total	Amount Paid
8281711482	1011906651	10-OCT-2023	**188,164.80 USD**	

Please put your Transaction Number and your Customer Account Number on your payment for prompt processing.

MASSACHUSETTS STATE POLICE
ATTN: Accounts Payable
470 WORCESTER RD
FRAMINGHAM MA 01702
United States

Payment Transfer Details

Bank of America, Dallas
WIRE Routing Transit Number: 026009593
ACH/EFT Routing Transit Number: 111000012
SWIFT: BOFAUS3N
Bank Account No: 3756319806

Send Payments To:

MOTOROLA SOLUTIONS
Motorola Solutions, Inc.
13108 Collections Center
Chicago IL 60693
United States
Please provide your remittance details to:
US.remittance@motorolasolutions.com

DIVERSION CONTRARY TO EXPORT CONTROL LAW IS PROHIBITED

MOTOROLA SOLUTIONS

ORIGINAL INVOICE

Motorola Solutions, Inc.
500 West Monroe
Chicago IL 60661
United States
Federal Tax ID: 36-1115800

Transaction Number	Transaction Date	Transaction Total
8281711482	10-SEP-2023	**188,164.80 USD**

P.O. Number	P.O. Date	Customer Account No
2024MOTRLU07POL20232	14-AUG-2023	1011906651

Payment Terms	Payment Due Date
Net Due in 30 Days	10-OCT-2023

Visit our website at www.motorolasolutions.com

Line Item #	Item Number	Description	Qty.	Unit Price (USD)	Amount (USD)
		Consisting of the following items			
	WGA00684	M5F FRONT CAMERA ASSY, W/ MOUNT, M500 **SERIAL NUMBERS** M5F1-009982 M5F1-010086 M5F1-010091 M5F1-010093 M5F1-010138 M5F1-010139 M5F1-010143 M5F1-010204 M5F1-010454 M5F1-010456 M5F1-019517 M5F1-019519 M5F1-019574 M5F1-019596 M5F1-019609 M5F1-019688 M5F1-019705 M5F1-019731 M5F1-019736 M5F1-019741 M5F1-019745 M5F1-019758 M5F1-019798 M5F1-019803	24	0.00	0.00
	WGA00690	M5P PASSENGER CAMERA ASSEMBLY, M500 **SERIAL NUMBERS** M5P1-012604 M5P1-012616 M5P1-012650 M5P1-012656 M5P1-012689 M5P1-012834 M5P1-012967 M5P1-012982 M5P1-013058 M5P1-013429 M5P1-013965 M5P1-014280 M5P1-014305 M5P1-014358 M5P1-014948 M5P1-016501 M5P1-016502 M5P1-016506 M5P1-016507 M5P1-016518 M5P1-016520 M5P1-016521 M5P1-016523 M5P1-016577	24	0.00	0.00
	WGA00635-KIT2	V300 WIFI DOCK VHCL CHGR/UPLD KIT FOR M500 W/O SPS	24	0.00	0.00
	WGA00675	ASSEMBLY, M5DDISPLAY **SERIAL NUMBERS** M5D1-004406 M5D1-004411 M5D1-004414 M5D1-004417 M5D1-004419 M5D1-004421 M5D1-004422 M5D1-004425 M5D1-004429 M5D1-004430 M5D1-004431 M5D1-004434 M5D1-004437 M5D1-004438 M5D1-023717 M5D1-023739 M5D1-023889 M5D1-023948 M5D1-023997 M5D1-024032 M5D1-024034 M5D1-024039 M5D1-024040 M5D1-024108	24	0.00	0.00
	WGA00790	ASSEMBLY, M5R REAR CAMERA, M500 **SERIAL NUMBERS** M5R1-004462 M5R1-004467 M5R1-004470 M5R1-004477 M5R1-004565 M5R1-004572 M5R1-004639 M5R1-004656 M5R1-004659 M5R1-004702 M5R1-004706 M5R1-004709 M5R1-004710 M5R1-004763 M5R1-004764 M5R1-004767 M5R1-004785 M5R1-004786 M5R1-004792 M5R1-004793 M5R1-004807 M5R1-004822 M5R1-004823 M5R1-004830	24	0.00	0.00
	WGA701CA-KIT	M500 INSTLL KIT CBL,BRKT,GPS,CABMIC,RCAM	24	0.00	0.00
	WGA00700	M500 ALPR DVR, 3 CAMS, 1080P, 1TB SSD **SERIAL NUMBERS** M500-001954 M500-002021 M500-002102 M500-002104 M500-002117 M500-002118 M500-002125 M500-002126 M500-002134 M500-002139 M500-002146 M500-002190 M500-020500 M500-020540 M500-020553 M500-020559 M500-020578 M500-020592 M500-020711 M500-020734 M500-020735 M500-020741 M500-020756 M500-020769	24	0.00	0.00
5	WGW00000	EXTENDED WARRANTY- FOR PERIPHERALS Service From: 09-SEP-2024 Service To: 08-SEP-2029	24	0.00	0.00
5.1	WGW00000	EXTENDED WARRANTY- FOR PERIPHERALS Service From: 09-SEP-2024 Service To: 08-SEP-2029	24	0.00	0.00
5.2	WGW00000	EXTENDED WARRANTY- FOR PERIPHERALS Service From: 09-SEP-2024 Service To: 08-SEP-2029	24	0.00	0.00
5.3	WGW00000	EXTENDED WARRANTY- FOR PERIPHERALS Service From: 09-SEP-2024 Service To: 08-SEP-2029	24	0.00	0.00
5.4	WAR-M500-CAR-2Y	M500 EXTENDED WARRANTY - 24 M500 ALPR DVR, 3 CAMS, 1080P, 1TB SSD: 09-SEP-24 - 08-SEP-29 Service From: 09-SEP-2024 Service To: 08-SEP-2029	24	1,215.20	29,164.80

DIVERSION CONTRARY TO EXPORT CONTROL LAW IS PROHIBITED

MOTOROLA SOLUTIONS

Motorola Solutions, Inc.
500 West Monroe
Chicago IL 60661
United States
Federal Tax ID: 36-1115800

Visit our website at www.motorolasolutions.com

ORIGINAL INVOICE

Transaction Number	Transaction Date	Transaction Total
8281711482	10-SEP-2023	**188,164.80 USD**

P.O. Number	P.O. Date	Customer Account No
2024MOTRLU07POL20232	14-AUG-2023	1011906651

Payment Terms	Payment Due Date
Net Due in 30 Days	10-OCT-2023

Line Item #	Item Number	Description	Qty.	Unit Price (USD)	Amount (USD)
		Tracking Number(s): 6672265261			
				USD Subtotal	**188,164.80**
				USD Total Tax	**0.00**
				USD Total	**188,164.80**
				USD Amount Due	**188,164.80**

DIVERSION CONTRARY TO EXPORT CONTROL LAW IS PROHIBITED

2815



MSP

Status report

Feb 10th

2816 Delivery Actions

- Completed:
  - Preventive Monitoring:
    - Scripts for monitoring storage and memory consumption with automatic restart (PAGIS microservice when the memory consumption is above 80% for example)
    - Scripts for monitoring the microservices restart – After implementing the Workaround, there have been no more service interruptions.
- Completed:
  - Improve memory monitoring of PAGIS micro-services for debugging purposes to allow us to identify which objects produce the memory leak problem
  - The delivery team is reviewing release 57 in the staging environment in order to deploy to MSP on Thursday 1/12 – Released on Thursday 1/19
    - Search screen - Increase search pagination from 15 to 60
    - Offline Notifications - Device offline notifications to include a "no reads received" option.
    - Reports - This to include bigger picture, Device, System and User time stamp.
    - Notification Sort - Profile sorting by Name
    - Time access filters - Ability to permission trim a user group to access only a certain amount of historical data, i.e., 24 hours or 30 days.
    - Addressed all of the issues above.

Copyright © 2021 Neology, All Rights Reserved.

Development

RC 58

Move to QA on 1/17 for the next 2 weeks
Resolve the 16 bugs:

- Read Search Filter Stops Working
- Devices Save Function Not Working
- Wildcard Searches Timing Out
- Device List Scroll Broken
- Filters randomly disappear

The RC is in QA and those reported on Friday Jan 20th will be added, which are:

- Aspect ratio in the image of the report
- Last modified field to update only when configuration changes
- Notification profile order - Hotlist names are not complete displayed

All the bugs reported are in the RC 58 (in QA)

RC 59

Start on 1/17 and ends on 1/27

Resolve the last 3 bugs:

- Mantis Day & Night filters
- Interoperability
- Mobile Covert hotlist

This concludes the bugs registered for MSP

- The Sprint has already started

All the bugs are in QA

RC60 to RC75

In each sprint the plan is to implement at least 2 requirements and enhancements to conclude the 26 tickets registered.

The plan is to finish at the beginning of October

In the RC 60 is added:
- Change the date component to one that allows typing editing
- Date and time are seen on top
- Hotlist screen date move when zooming
- In the read report the text will be changed so that it is not doubly denied

- RC 60 - In progress

The plan is to deploy a new release every two months starting in March with the version that closes the 8 (plus 8 that are added with the feedback received on Friday Jan 20th) bugs open at this point.

Copyright © 2021 Neology, All Rights Reserved.

Release plan (Bugs) - updated Feb 3rd

2818

Summary	Priority	Status	Created	Issue Type	Updated	Fix version	End Date	QA	Staging	Release Date
Read Detail Report - image aspect radio is not dis	Medium	Done	23/01/23 1	Bug	24/01/23 1	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Hotlists: last modification date is not longer a vali	Medium	In Progress	23/01/23 1	Bug	23/01/23 2	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Notification page layout- big hotlist name not full	Medium	Done	23/01/23 1	Bug	23/01/23 2	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Notification sorting - profiles names with a space	Medium	Done	23/01/23 1	Bug	23/01/23 2	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Read Search Filter Stops Working	Highest	Done	09/01/23 2	Bug	23/01/23 2	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Devices Save Function Not Working - Hotlist Deplo	Highest	For Approv	06/01/23 1	Bug	19/01/23 5	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Wildcard Searches Timing Out	Highest	Done	06/01/23 1	Bug	13/01/23 1	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Device List Scroll Broken	Highest	Done	06/01/23 1	Bug	23/01/23 2	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Filters randomly disappear	Highest	Done	06/01/23 1	Bug	11/01/23 2	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Mantis - Mantis Day & Night filters	Highest	Done	09/01/23 2	Bug	13/01/23 1	RC 59	27/01/23	10/02/23	17/02/23	06/03/23
Interoperability	Highest	For Approv	09/01/23 1	Bug	19/01/23 5	RC 59	27/01/23	10/02/23	17/02/23	06/03/23
Mobile Covert hotlist	Highest	Done	09/01/23 1	Bug	12/01/23 1	RC 59	27/01/23	10/02/23	17/02/23	06/03/23
Arrows in main hotlist depending on zoom stop w	Medium	Done	23/01/23 1	Bug	23/01/23 2	RC 59	27/01/23	10/02/23	17/02/23	06/03/23
Read Detail Report:¬† the NTP double negative	Medium	Done	23/01/23 1	Bug	23/01/23 1	RC 59	27/01/23	10/02/23	17/02/23	06/03/23
Search time & date filter start/end times no longe	Medium	In Progress	23/01/23 1	Bug	24/01/23 1	RC 59	27/01/23	10/02/23	17/02/23	06/03/23
Search time & date filter overlap with calendar bu	Medium	Done	23/01/23 1	Bug	24/01/23 1	RC 59	27/01/23	10/02/23	17/02/23	06/03/23

Copyright © 2021 Neology, All Rights Reserved.

2819

Release plan (New Features) - updated Feb 3rd

Summary	Priority	Status	Created	Issue Type	Updated	Fix versions	End Date	QA	Staging	Release Date
Filters - change name	Highest	Done	10/01/23 17:47	Task	02/02/23 20:20	RC 60	10/03/23	24/03/23	31/03/23	02/05/23
Hotlist - Auto-notification of hotlist and hc	Highest	In Progress	10/01/23 17:43	Story	02/02/23 18:17	RC 60	10/03/23	24/03/23	31/03/23	02/05/23
Reports-Global day	Highest	To Do	10/01/23 17:41	Task	11/01/23 21:00	RC 60	10/03/23	24/03/23	31/03/23	02/05/23
Suspicious Traveler	Highest	In Progress	10/01/23 17:39	Task	31/01/23 23:24	RC 60	10/03/23	24/03/23	31/03/23	02/05/23
Search- improvement in the front end	Highest	For Approval	10/01/23 17:38	Story	31/01/23 16:30	RC 60	10/03/23	24/03/23	31/03/23	02/05/23
Filters - change the name of the filter "br	Highest	Done	10/01/23 17:50	Task	31/01/23 18:32	RC 61	24/03/23	07/04/23	14/04/23	02/05/23
Hotlist - change name	Highest	To Do	10/01/23 17:49	Task	31/01/23 23:08	RC 61	10/03/23	24/03/23	31/03/23	02/05/23
Group setting- permission by device	Highest	To Do	10/01/23 17:45	Story	02/02/23 18:19	RC 61	10/03/23	24/03/23	31/03/23	02/05/23
BOSS covert hotlist	Highest	To Do	10/01/23 17:51	Task	11/01/23 15:00	RC 62	07/04/23	21/04/23	28/04/23	03/07/23
Mantis - add AND or OR possibility	Highest	To Do	10/01/23 18:23	Story	31/01/23 18:26	RC 62	07/04/23	21/04/23	28/04/23	03/07/23
Dashboard - new permission to visualize t	Highest	To Do	10/01/23 17:54	Task	11/01/23 16:26	RC 63	07/04/23	21/04/23	28/04/23	03/07/23
Filters- turn off specific filters	Highest	To Do	10/01/23 17:56	Task	11/01/23 16:26	RC 64	21/04/23	05/05/23	12/05/23	03/07/23
Multi-reads/hit report NTP Fields	Medium	To Do	11/01/23 20:29	Task	11/01/23 22:53	RC 65	05/05/23	19/05/23	26/05/23	03/07/23
Multi-reads/hit report sort	Medium	To Do	11/01/23 20:22	Task	11/01/23 22:53	RC 65	05/05/23	19/05/23	26/05/23	03/07/23
Hotlist - Criteria of the hotlist	Highest	To Do	10/01/23 17:59	Story	31/01/23 18:30	RC 65	05/05/23	19/05/23	26/05/23	03/07/23
Reports show Hotlist expiration date	Medium	To Do	11/01/23 20:14	Task	11/01/23 22:53	RC 66	19/05/23	02/06/23	09/06/23	03/07/23
Hotlist- improvement in the hotplate front	Highest	To Do	10/01/23 18:09	Story	31/01/23 18:28	RC 66	19/05/23	02/06/23	09/06/23	03/07/23
Permission search filters	Medium	To Do	11/01/23 20:31	Task	11/01/23 22:53	RC 67	02/06/23	16/06/23	23/06/23	04/09/23
Caravans	Highest	To Do	10/01/23 18:13	Story	31/01/23 18:27	RC 67	02/06/23	16/06/23	23/06/23	04/09/23
add a new opcion of 2FA	Highest	To Do	10/01/23 18:11	Story	11/01/23 16:27	RC 68	16/06/23	30/06/23	07/07/23	04/09/23
Multi-reads/hit report Overview Image	Medium	To Do	11/01/23 20:26	Task	11/01/23 22:53	RC 69	30/06/23	14/07/23	21/07/23	04/09/23
Filters - remove op shot sticker	Highest	To Do	10/01/23 18:14	Story	11/01/23 16:28	RC 69	30/06/23	14/07/23	21/07/23	04/09/23
Notifications- add a third app	Highest	To Do	10/01/23 18:18	Story	11/01/23 16:29	RC 70	14/07/23	28/07/23	04/08/23	04/09/23
notifications - intuitive improvements	Highest	To Do	10/01/23 18:22	Story	31/01/23 18:55	RC 72	28/07/23	11/08/23	18/08/23	04/09/23
State Match NCIC Hits	Highest	To Do	10/01/23 18:26	Story	11/01/23 17:46	RC 74	11/08/23	25/08/23	01/09/23	04/09/23
Hotlist NCIC state is not correct	Highest	To Do	09/01/23 20:01	Story	11/01/23 17:46	RC 74	11/08/23	25/08/23	01/09/23	02/10/23
IOS App	Highest	To Do	11/01/23 14:38	Story	11/01/23 16:31	RC 75	25/08/23	08/09/23	15/09/23	02/10/23

Copyright © 2021 Neology, All Rights Reserved.

Release plan (Bugs Pagis) - updated Feb 10

2820

Summary	Priority	Status	Type	Version	Release Date
Delayed Login due to hotlist purge cycle. • This would also cause missing hotlist. • Very long delays at login.	Medium	Released	Bug	2.15.2.12	1/25/23
Hotlist Overflow database. • Special characters in Hotlist names causing exceptions in PAGIS.	Medium	Released	Bug	2.15.2.12	1/25/23
PAGIS crashing. • Due to large number of hotlist and hotplates.	High	Released	Bug	2.15.2.12	1/25/23
Black & white image in overview. • Caused when color capture is enabled.	High	Released	Bug	2.15.2.12	1/25/23
Windows display scaling effects. • Causing OCR and Overview image to be clipping.	Medium	Released	Bug	2.15.2.12	1/25/23
Inconsistent and random GPS coordinates, including random characters in S/N watermark.	High	Q/A Testing	Bug	2.15.2.13	2/27/2023
Alert delays. • Caused by PAGIS duplicating hotplates in the database. • This would also cause delayed hit notifications. • General slowness in the system.	High	Released	Bug	2.15.2.11	1/03/23

Copyright © 2021 Neology, All Rights Reserved.

2821



Thank you

Copyright © 2021 Neology, All Rights Reserved.

2822



MSP

Status report

March 6th

2823 Delivery Actions

- Completed:
  - Preventive Monitoring:
    - Scripts for monitoring storage and memory consumption with automatic restart (PAGIS microservice when the memory consumption is above 80% for example)
    - Scripts for monitoring the microservices restart – After implementing the Workaround, there have been no more service interruptions.
  - The delivery team is reviewing release 57 in the staging environment in order to deploy to MSP on Thursday 1/12 – Released on Thursday 1/19
    - Search screen - Increase search pagination from 15 to 60
    - Offline Notifications - Device offline notifications to include a "no reads received" option.
    - Reports - This to include bigger picture, Device, System and User time stamp.
    - Notification Sort - Profile sorting by Name
    - Time access filters - Ability to permission trim a user group to access only a certain amount of historical data, i.e., 24 hours or 30 days.
    - Addressed all of the issues above.
  - Release 58
    - Improve memory monitoring of PAGIS micro-services for debugging purposes to allow us to identify which objects produce the memory leak problem (in QA with RC58)
    - RC58 was deployed in Staging and Demo environments (3/2)
  - In progress:
    - During March 6 and 7, the deployment in MSP (Scripts and Database update) will be prepared.
    - The version will be deployed in MSP on Wednesday the 8th at night.
    - The RC60 is in progress (It is planned to release in May)

Copyright © 2021 Neology, All Rights Reserved.

Development

2824



RC 58

Resolve the 15 bugs:

- Read Search Filter Stops Working
- Devices Save Function Not Working
- Wildcard Searches Timing Out
- Device List Scroll Broken
- Filters randomly disappear
- Aspect ratio in the image of the report
- Last modified field to update only when configuration changes
- Notification profile order - Hotlist names are not complete displayed
- Mantis Day & Night filters
- Interoperability
- Mobile Covert hotlist
- Change the date component to one that allows typing editing
- Date and time are seen on top
- Hotlist screen date move when zooming
- In the read report the text will be changed so that it is not doubly denied

The release Is now in QA



RC 60

Planned to be deployed in May 2023

In progress:
- Hotlist Auto-notification
- Reads visibility based on permits and roles
- Improve in suspicious traveller

To-Do:
- Reports Total Day
- Change name of filters
- Search improvements
- Improvements on Hotlist Frontend



RC61 to RC75

In each sprint the plan is to implement at least 2 requirements and enhancements to conclude the 26 tickets registered.

The plan is to finish at the beginning of October 2023.

Note: RC58 and RC59 were merged.

RC58 in procees to be deploye this week.

Copyright © 2021 Neology, All Rights Reserved.

Release plan (Bugs) - updated 3/5

2825

Summary	Priority	Status	Created	Issue Type	Updated	Fix Version	End Date	QA	Staging	Release Date
Interoperability - SF76691	Highest	Done	10/01/23	Bug	02/02/23	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Search time & date filter start/end times no longer allow typed in t	Medium	Done	11/01/23	Bug	02/02/23	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Read Detail Report - image aspect radio is not displayed correctly	Medium	Done	12/01/23	Bug	11/01/23	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Notification page layout- big hotlist name not full display	Medium	Done	13/01/23	Bug	31/01/23	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Notification sorting - profiles names with a space	Medium	Done	14/01/23	Bug	31/01/23	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Read Search Filter Stops Working	Highest	Done	15/01/23	Bug	31/01/23	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Wildcard Searches Timing Out	Highest	Done	16/01/23	Bug	31/01/23	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Device List Scroll Broken	Highest	Done	17/01/23	Bug	02/02/23	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Filters randomly disappear	Highest	Done	18/01/23	Bug	11/01/23	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Mantis - Mantis Day & Night filters	Highest	Done	19/01/23	Bug	31/01/23	RC 58	27/01/23	10/02/23	17/02/23	06/03/23
Arrows in main hotlist depending on zoom stop working	Medium	Done	20/01/23	Bug	11/01/23	RC 58	27/01/23	10/02/23	17/02/23	06/03/23
Read Detail Report:¬† the NTP double negative	Medium	Done	21/01/23	Bug	11/01/23	RC 58	27/01/23	10/02/23	17/02/23	06/03/23
Search time & date filter overlap with calendar button	Medium	Done	22/01/23	Bug	11/01/23	RC 58	27/01/23	10/02/23	17/02/23	06/03/23
Mobile Covert hotlist	Highest	Closed	23/01/23	Bug	31/01/23	RC 58	27/01/23	10/02/23	17/02/23	06/03/23
Hotlists: last modification field changes when hotsources are updat	Medium	Not replicated	24/01/23	Bug	11/01/23	RC 58	27/01/23	10/02/23	17/02/23	06/03/23
Devices Save Function Not Working - Hotlist Deployment	Highest	Done	25/01/23	Bug	31/01/23	RC 58	27/01/23	10/02/23	17/02/23	06/03/23

Copyright © 2021 Neology, All Rights Reserved.

QA Bugs – updated 3/5

2826

Summary	Priority	Status	Created	Issue Type	Updated	Fix Version	End Date	QA	Staging	Release Date
Remote server cannot see mantis filter	2.-High	Done	24/02/23	Bug	02/02/23	RC 58	27/02/23	28/01/23	03/02/23	06/03/23
Summary report is not created	2.-High	Done	25/02/23	Bug	02/02/23	RC 58	27/02/23	28/01/23	03/02/23	06/03/23
Includes and excludes must not be case sensitive	2.-High	Done	26/02/23	Bug	11/01/23	RC 58	27/02/23	28/01/23	03/02/23	06/03/23
PAGIS is missing a lot of hotplates with sync	2.-High	Done	27/02/23	Bug	31/01/23	RC 58	27/02/23	28/01/23	03/02/23	06/03/23
Hotlist from a group are not assigned to a user	3.-Medium	Done	28/02/23	Bug	31/01/23	RC 58	27/02/23	28/01/23	03/02/23	06/03/23
Reads don't appear until user scrolling down	3.-Medium	Done	01/03/23	Bug	31/01/23	RC 58	27/02/23	28/01/23	03/02/23	06/03/23

The development team compromise to solve them on Monday the 27th and no later than Tuesday the 28th.

Copyright © 2021 Neology, All Rights Reserved.

2827

Release plan (New Features) - updated Feb 17th

Summary	Priority	Status	Created	Issue Type	Updated	Fix versions	End Date	QA	Staging	Release Date
Filters - change name	Highest	Done	10/01/23 17:47	Task	02/02/23 20:20	RC 60	10/03/23	24/03/23	31/03/23	02/05/23
Hotlist - Auto-notification of hotlist and hot pla	Highest	In Progress	10/01/23 17:43	Story	02/02/23 18:17	RC 60	10/03/23	24/03/23	31/03/23	02/05/23
Reports-Global day	Highest	To Do	10/01/23 17:41	Task	11/01/23 21:00	RC 60	10/03/23	24/03/23	31/03/23	02/05/23
Suspicious Traveler	Highest	In Progress	10/01/23 17:39	Task	31/01/23 23:24	RC 60	10/03/23	24/03/23	31/03/23	02/05/23
Search- improvement in the front end	Highest	For Approval	10/01/23 17:38	Story	31/01/23 16:30	RC 60	10/03/23	24/03/23	31/03/23	02/05/23
Filters - change the name of the filter "brand"	Highest	Done	10/01/23 17:50	Task	31/01/23 18:32	RC 61	24/03/23	07/04/23	14/04/23	02/05/23
Hotlist - change name	Highest	To Do	10/01/23 17:49	Task	31/01/23 23:08	RC 61	10/03/23	24/03/23	31/03/23	02/05/23
Group setting- permission by device	Highest	In Progress	10/01/23 17:45	Story	02/02/23 18:19	RC 61	10/03/23	24/03/23	31/03/23	02/05/23
BOSS covert hotlist	Highest	To Do	10/01/23 17:51	Task	11/01/23 15:00	RC 62	07/04/23	21/04/23	28/04/23	03/07/23
Mantis - add AND or OR possibility	Highest	To Do	10/01/23 18:23	Story	31/01/23 18:26	RC 62	07/04/23	21/04/23	28/04/23	03/07/23
Dashboard - new permission to visualize the da	Highest	To Do	10/01/23 17:54	Task	11/01/23 16:26	RC 63	07/04/23	21/04/23	28/04/23	03/07/23
Filters- turn off specific filters	Highest	To Do	10/01/23 17:56	Task	11/01/23 16:26	RC 64	21/04/23	05/05/23	12/05/23	03/07/23
Multi-reads/hit report NTP Fields	Medium	To Do	11/01/23 20:29	Task	11/01/23 22:53	RC 65	05/05/23	19/05/23	26/05/23	03/07/23
Multi-reads/hit report sort	Medium	To Do	11/01/23 20:22	Task	11/01/23 22:53	RC 65	05/05/23	19/05/23	26/05/23	03/07/23
Hotlist - Criteria of the hotlist	Highest	To Do	10/01/23 17:59	Story	31/01/23 18:30	RC 65	05/05/23	19/05/23	26/05/23	03/07/23
Reports show Hotlist expiration date	Medium	To Do	11/01/23 20:14	Task	11/01/23 22:53	RC 66	19/05/23	02/06/23	09/06/23	03/07/23
Hotlist- improvement in the hotplate front end	Highest	To Do	10/01/23 18:09	Story	31/01/23 18:28	RC 66	19/05/23	02/06/23	09/06/23	03/07/23
Permission search filters	Medium	To Do	11/01/23 20:31	Task	11/01/23 22:53	RC 67	02/06/23	16/06/23	23/06/23	04/09/23
Caravans	Highest	To Do	10/01/23 18:13	Story	31/01/23 18:27	RC 67	02/06/23	16/06/23	23/06/23	04/09/23
add a new opcion of 2FA	Highest	To Do	10/01/23 18:11	Story	11/01/23 16:27	RC 68	16/06/23	30/06/23	07/07/23	04/09/23
Multi-reads/hit report Overview Image	Medium	To Do	11/01/23 20:26	Task	11/01/23 22:53	RC 69	30/06/23	14/07/23	21/07/23	04/09/23
Filters - remove op shot sticker	Highest	To Do	10/01/23 18:14	Story	11/01/23 16:28	RC 69	30/06/23	14/07/23	21/07/23	04/09/23
Notifications- add a third app	Highest	To Do	10/01/23 18:18	Story	11/01/23 16:29	RC 70	14/07/23	28/07/23	04/08/23	04/09/23
notifications - intuitive improvements	Highest	To Do	10/01/23 18:22	Story	31/01/23 18:55	RC 72	28/07/23	11/08/23	18/08/23	04/09/23
State Match NCIC Hits	Highest	To Do	10/01/23 18:26	Story	11/01/23 17:46	RC 74	11/08/23	25/08/23	01/09/23	04/09/23
Hotlist NCIC state is not correct	Highest	To Do	09/01/23 20:01	Story	11/01/23 17:46	RC 74	11/08/23	25/08/23	01/09/23	02/10/23
IOS App	Highest	To Do	11/01/23 14:38	Story	11/01/23 16:31	RC 75	25/08/23	08/09/23	15/09/23	02/10/23

Copyright © 2021 Neology, All Rights Reserved.

Release plan (Bugs Pagis) - updated 3/5

2828

Summary	Priority	Status	Type	Version	Release Date
Delayed Login due to hotlist purge cycle. • This would also cause missing hotlist. • Very long delays at login.	Medium	Released	Bug	2.15.2.12	1/25/23
Hotlist Overflow database. • Special characters in Hotlist names causing exceptions in PAGIS.	Medium	Released	Bug	2.15.2.12	1/25/23
PAGIS crashing. • Due to large number of hotlist and hotplates.	High	Released	Bug	2.15.2.12	1/25/23
Black & white image in overview. • Caused when color capture is enabled.	High	Released	Bug	2.15.2.12	1/25/23
Windows display scaling effects. • Causing OCR and Overview image to be clipping.	Medium	Released	Bug	2.15.2.12	1/25/23
Inconsistent and random GPS coordinates, including random characters in S/N watermark.	High	Released	Bug	2.15.2.13	2/27/23
Alert delays. • Caused by PAGIS duplicating hotplates in the database. • This would also cause delayed hit notifications. • General slowness in the system.	High	In Q&A by Michael Roth	Bug	2.15.2.14	1/03/23
• Covert Hotlist Showing Hits	High	In Q&A by Michael Roth	Bug	2.15.2.15	2/24/23 3/3/23 – Installer released to MRoth

Copyright © 2021 Neology, All Rights Reserved.

- PAGIS Release 2.15.2.14
  - Released to QA on Febrary 20th
  - Fixes included in this version:
    - NTPStatusLocked flag behavior for MDC was fixed.
    - Default US Datetime format
    - Alert sound is still played when Mute option in PAGIS is enabled
    - Delay when closing session was fixed
    - Delay when saving sync settings was fixed
- In progress (next release:
  - Covert hotlist is showing & sounding hits in single pane mode, Dual screen mode plays hit sound. expected behavior it to show no signs of hits from covert hotlist. (Reported 2/22)

Copyright © 2021 Neology, All Rights Reserved.

Q&A Process

2830

- The immediate actions are:
  - Review the unit testing process – in progress (March 15th)
  - Re-implement a peer code review process on the development team – in progress (February 28th)
  - Implement load and stress tests for each release – in progress (March 31th)
    - First Load and Stress test is in progress during this week 2/27
  - Review in detail the manual testing process – in progress (April 30th)
  - Review in detail the automatic testing process – in progress (April 30th)
  - Perform a root cause analysis of each error that reaches production - Done
  - Add usability test for every change in UI – Completed (February 15th)

Copyright © 2021 Neology, All Rights Reserved.

SX4e[2831] Hardware / RMA

- Deep dive analysis on SX4e RMA's is on-going;
- Initial analysis shows no immediate / obvious clustering of same source
  - Dead CMOS Battery; Power Cable Shorted; Win10 Image issues

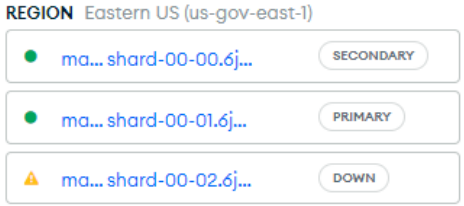
- Current recommendation is to ensure all units are running latest Software image (at least upgrade from NE220311 to NE220701 image)

- As interim, in addition to Service Spares already provided to MSP, an additional SX4e (with current imaging, extended production soak etc) shall be provided as hot spare to MSP to minimize Mobile Unit downtime.

Copyright © 2021 Neology, All Rights Reserved.

1/24[2832] – Incident Overview - Closed

- Partial Outage of BOSS4 User-Interface with degraded service caused by one (of three) nodes being unresponsive
- Impact was seen on one microservice (API Gateway) linked to User Interface although all other parts of the system continued to function. No additional impact since 1/24.
- Automatic restarts and reconnection is built into this part of the system however continued instability resulted in manual intervention by Neology Tech Support team
- Total length of incident from initial automated activity through to restoration and completion of system health checks was 1hr 41min.
- On-going analysis of log files continues – initial analysis noted Node/Cluster restarts and rebalancing. Involving 3rd line team in analysis
- Suggestion made that where user interruption / outage is noted that Neology is provided with MSP User Email Group so notifications can be sent out to avoid users routing via Noah.
- Actions
  - Today 1/25 The incident will continue to be analyzed by the Solutions Delivery team
  - The case with Mongo will also be escalated because the incident occurred on the database side. Tech support case was created (1081)
  - An improvement in monitoring will be analyzed and implemented to identify this case in a more timely and automatic manner (Feb 10th). In deployment, additional scripts created to manage the log files.
  - The micro-service will be improved so that if the connection to the default node of the database cluster fails, it will try it with the next one (will be released with RC60 in May).



Copyright © 2021 Neology, All Rights Reserved.

QA IN DEVELOPMENT PROCESS

2833

neology

Definitions	Share with the team	Start coding	Send to develop environment	Internal Test (New)
STEP1	STEP2	STEP3	STEP4	STEP5
				
1- Meetings with Product Owner 2- Create tickets on Jira 3-Create documents requirements/user stories	1- Internal meeting with develop team 2- Share documentation: • jira ticket • Requirements • User stories • Criteria of acceptance	1- Analyze the requirement 2-Modify existing code or create new branches 3- Develop unit test	1-Pull request to send to dev 2- Peer code review process 3- Sonar scan	1- Validate the changes based on acceptance criteria 2- End user testing by our UX Designer
			In the peer code review process the other developers review the new code and validate if the code is secure, correct, good practices are followed if the new code is approved with the CI CD process the changes are injected to dev	
Still working in reimplement unit testing scope	Sonar is a tool that scan the last changes to search vulnerabilities in the code if sonar does not find problems with the change the push is correctly integrated on dev		Now only back end developers can approve the back end changes and front end changes only can be approve by front end developers (new)	

Copyright © 2021 Neology, All Rights Reserved. Company Proprietary.

QA PROCESS 2834

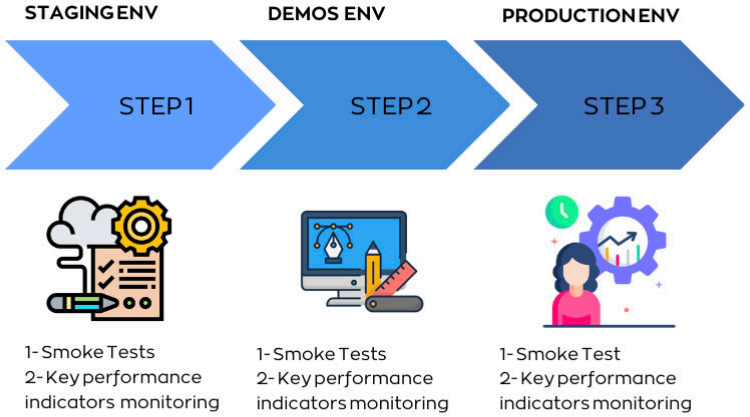
Duration 2 weeks

PREPARATION	MATRIX DESIGN	TEST EXECUTION	SHARE TEST RESTULTS	CONFIRMATION TEST
STEP1	STEP2	STEP3	STEP4	STEP5
				
1- Meeting with develop team sprint review	1- Internal meeting with qa team 2- Select the test cases 3-Design test cases	1-Assign test cases 2-Execute automated cases 3- Execute manual cases During sprint they did a complete cicle and a regression cicle: **Automated** 226 (of 353) **Manual Test** 302 (of 591) **Total general** 528 (of 944)	1-Create jira tickets if they detect an issue 2-Share with the develop team the issues discovered In the last process they discover (at 2/24): **Highest -0** **High. -4** **Medium. -2** **Low -17** **Very Low-3** Note: very high, high and medium defects must be solved to send the version to a production company	1- Close the graphs of the results 2- Shared the results by an email confirmation with the last results

Note: no all test cases were executed because the version dont affect all the modules in the system

Copyright © 2021 Neology, All Rights Reserved. Company Proprietary.

QA IN DELIVERY PROCESS

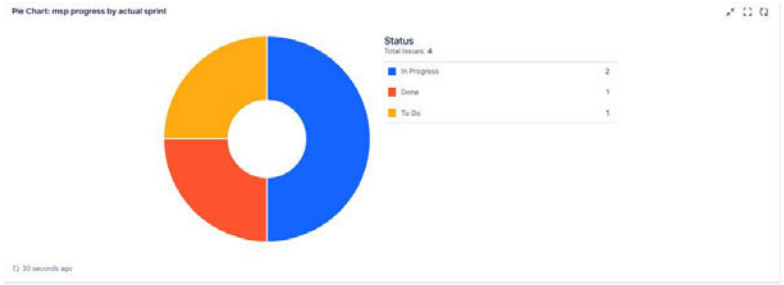


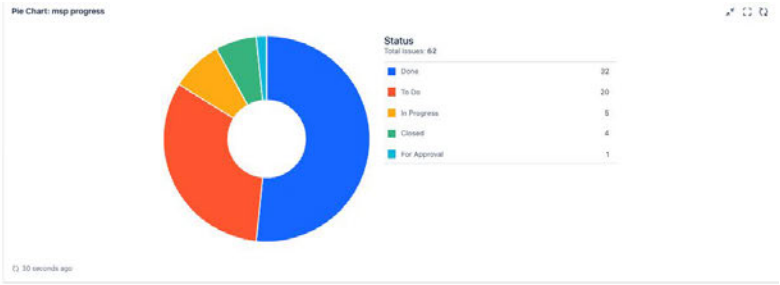
Smoke test: cover the most important functionalities int he system

Copyright © 2021 Neology, All Rights Reserved. Company Proprietary.

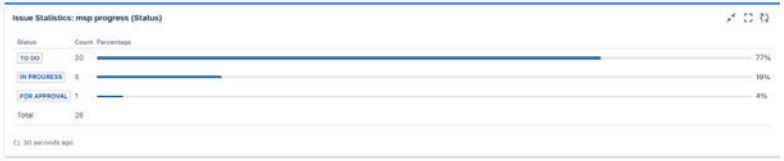
2836

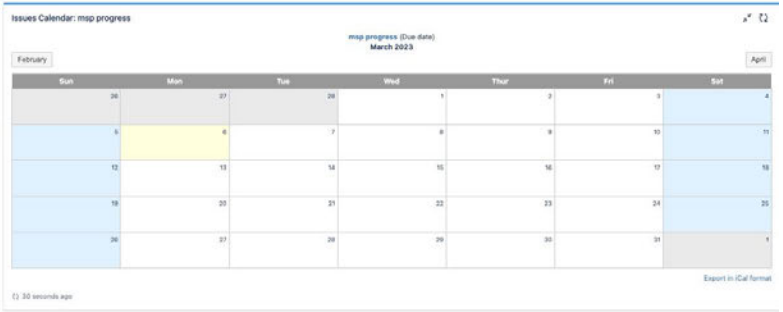
Dashboard -updated Feb 27th

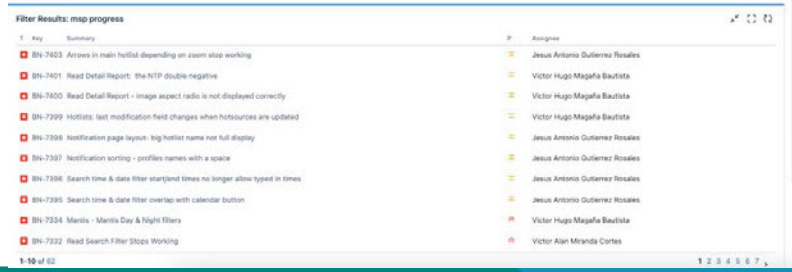












Copyright © 2021 Neology, All Rights Reserved.

2837



Thank you

Copyright © 2021 Neology, All Rights Reserved.

2838



MSP

Status report

Feburary 22nd

2839 Delivery Actions

- Completed:
  - Preventive Monitoring:
    - Scripts for monitoring storage and memory consumption with automatic restart (PAGIS microservice when the memory consumption is above 80% for example)
    - Scripts for monitoring the microservices restart – After implementing the Workaround, there have been no more service interruptions.
  - The delivery team is reviewing release 57 in the staging environment in order to deploy to MSP on Thursday 1/12 – Released on Thursday 1/19
    - Search screen - Increase search pagination from 15 to 60
    - Offline Notifications - Device offline notifications to include a "no reads received" option.
    - Reports - This to include bigger picture, Device, System and User time stamp.
    - Notification Sort - Profile sorting by Name
    - Time access filters - Ability to permission trim a user group to access only a certain amount of historical data, i.e., 24 hours or 30 days.
    - Addressed all of the issues above.
- In progress:
  - Improve memory monitoring of PAGIS micro-services for debugging purposes to allow us to identify which objects produce the memory leak problem (in QA with RC58)
  - Release 58 is in QA planned to deployment on Monday March 6th (Detail in the next slide)

Copyright © 2021 Neology, All Rights Reserved.

Development

2840

RC 58

Resolve the 15 bugs:

- Read Search Filter Stops Working
- Devices Save Function Not Working
- Wildcard Searches Timing Out
- Device List Scroll Broken
- Filters randomly disappear
- Aspect ratio in the image of the report
- Last modified field to update only when configuration changes
- Notification profile order - Hotlist names are not complete displayed
- Mantis Day & Night filters
- Interoperability
- Mobile Covert hotlist
- Change the date component to one that allows typing editing
- Date and time are seen on top
- Hotlist screen date move when zooming
- In the read report the text will be changed so that it is not doubly denied

The release Is now in QA

RC 60

Planned to be deployed in May 2023

In progress:
- Hotlist Auto-notification
- Reads visibility based on permits and roles
- Improve in suspicious traveller

To-Do:
- Reports Total Day
- Change name of filters
- Search improvements
- Improvements on Hotlist Frontend

RC61 to RC75

In each sprint the plan is to implement at least 2 requirements and enhancements to conclude the 26 tickets registered.

The plan is to finish at the beginning of October 2023.

Note: RC58 and RC59 were merged.

- RC 59 has been incorporated into RC 58
- March Release (RC58) will close the 15 bugs reported.

Copyright © 2021 Neology, All Rights Reserved.

Release plan (Bugs) - updated Feb 17th

2841

Summary	Priority	Status	Created	Issue Type	Updated	Fix Version	End Date	QA	Staging	Release Date
Interoperability - SF766	Highest	For Approval	10/01/23 17:47	Bug	02/02/23 20:20	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Search time & date filte	Medium	For Approval	11/01/23 17:47	Bug	02/02/23 18:17	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Read Detail Report - in	Medium	Done	12/01/23 17:47	Bug	11/01/23 21:00	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Notification page layou	Medium	Done	13/01/23 17:47	Bug	31/01/23 23:24	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Notification sorting - pr	Medium	Done	14/01/23 17:47	Bug	31/01/23 16:30	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Read Search Filter Stop	Highest	Done	15/01/23 17:47	Bug	31/01/23 18:32	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Wildcard Searches Timi	Highest	Done	16/01/23 17:47	Bug	31/01/23 23:08	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Device List Scroll Broke	Highest	Done	17/01/23 17:47	Bug	02/02/23 18:19	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Filters randomly disapp	Highest	Done	18/01/23 17:47	Bug	11/01/23 15:00	RC 58	24/01/23	27/01/23	03/02/23	06/03/23
Mantis - Mantis Day & I	Highest	Done	19/01/23 17:47	Bug	31/01/23 18:26	RC 58	27/01/23	10/02/23	17/02/23	06/03/23
Arrows in main hotlist d	Medium	Done	20/01/23 17:47	Bug	11/01/23 16:26	RC 58	27/01/23	10/02/23	17/02/23	06/03/23
Read Detail Report:¬† t	Medium	Done	21/01/23 17:47	Bug	11/01/23 16:26	RC 58	27/01/23	10/02/23	17/02/23	06/03/23
Search time & date filte	Medium	Done	22/01/23 17:47	Bug	11/01/23 22:53	RC 58	27/01/23	10/02/23	17/02/23	06/03/23
Mobile Covert hotlist	Highest	Closed	23/01/23 17:47	Bug	31/01/23 18:30	RC 58	27/01/23	10/02/23	17/02/23	06/03/23
Hotlists: last modificati	Medium	Not replicated	24/01/23 17:47	Bug	11/01/23 22:53	RC 58	27/01/23	10/02/23	17/02/23	06/03/23
Devices Save Function N	Highest	For Approval	25/01/23 17:47	Bug	31/01/23 18:28	RC 58	27/01/23	10/02/23	17/02/23	06/03/23

Copyright © 2021 Neology, All Rights Reserved.

2842

Release plan (New Features) - updated Feb 17th

Summary	Priority	Status	Created	Issue Type	Updated	Fix versions	End Date	QA	Staging	Release Date
Filters - change name	Highest	Done	10/01/23 17:47	Task	02/02/23 20:20	RC 60	10/03/23	24/03/23	31/03/23	02/05/23
Hotlist - Auto-notification of hotlist and hot pla	Highest	In Progress	10/01/23 17:43	Story	02/02/23 18:17	RC 60	10/03/23	24/03/23	31/03/23	02/05/23
Reports-Global day	Highest	To Do	10/01/23 17:41	Task	11/01/23 21:00	RC 60	10/03/23	24/03/23	31/03/23	02/05/23
Suspicious Traveler	Highest	In Progress	10/01/23 17:39	Task	31/01/23 23:24	RC 60	10/03/23	24/03/23	31/03/23	02/05/23
Search- improvement in the front end	Highest	For Approval	10/01/23 17:38	Story	31/01/23 16:30	RC 60	10/03/23	24/03/23	31/03/23	02/05/23
Filters - change the name of the filter "brand"	Highest	Done	10/01/23 17:50	Task	31/01/23 18:32	RC 61	24/03/23	07/04/23	14/04/23	02/05/23
Hotlist - change name	Highest	To Do	10/01/23 17:49	Task	31/01/23 23:08	RC 61	10/03/23	24/03/23	31/03/23	02/05/23
Group setting- permission by device	Highest	In Progress	10/01/23 17:45	Story	02/02/23 18:19	RC 61	10/03/23	24/03/23	31/03/23	02/05/23
BOSS covert hotlist	Highest	To Do	10/01/23 17:51	Task	11/01/23 15:00	RC 62	07/04/23	21/04/23	28/04/23	03/07/23
Mantis - add AND or OR possibility	Highest	To Do	10/01/23 18:23	Story	31/01/23 18:26	RC 62	07/04/23	21/04/23	28/04/23	03/07/23
Dashboard - new permission to visualize the da	Highest	To Do	10/01/23 17:54	Task	11/01/23 16:26	RC 63	07/04/23	21/04/23	28/04/23	03/07/23
Filters- turn off specific filters	Highest	To Do	10/01/23 17:56	Task	11/01/23 16:26	RC 64	21/04/23	05/05/23	12/05/23	03/07/23
Multi-reads/hit report NTP Fields	Medium	To Do	11/01/23 20:29	Task	11/01/23 22:53	RC 65	05/05/23	19/05/23	26/05/23	03/07/23
Multi-reads/hit report sort	Medium	To Do	11/01/23 20:22	Task	11/01/23 22:53	RC 65	05/05/23	19/05/23	26/05/23	03/07/23
Hotlist - Criteria of the hotlist	Highest	To Do	10/01/23 17:59	Story	31/01/23 18:30	RC 65	05/05/23	19/05/23	26/05/23	03/07/23
Reports show Hotlist expiration date	Medium	To Do	11/01/23 20:14	Task	11/01/23 22:53	RC 66	19/05/23	02/06/23	09/06/23	03/07/23
Hotlist- improvement in the hotplate front end	Highest	To Do	10/01/23 18:09	Story	31/01/23 18:28	RC 66	19/05/23	02/06/23	09/06/23	03/07/23
Permission search filters	Medium	To Do	11/01/23 20:31	Task	11/01/23 22:53	RC 67	02/06/23	16/06/23	23/06/23	04/09/23
Caravans	Highest	To Do	10/01/23 18:13	Story	31/01/23 18:27	RC 67	02/06/23	16/06/23	23/06/23	04/09/23
add a new opcion of 2FA	Highest	To Do	10/01/23 18:11	Story	11/01/23 16:27	RC 68	16/06/23	30/06/23	07/07/23	04/09/23
Multi-reads/hit report Overview Image	Medium	To Do	11/01/23 20:26	Task	11/01/23 22:53	RC 69	30/06/23	14/07/23	21/07/23	04/09/23
Filters - remove op shot sticker	Highest	To Do	10/01/23 18:14	Story	11/01/23 16:28	RC 69	30/06/23	14/07/23	21/07/23	04/09/23
Notifications- add a third app	Highest	To Do	10/01/23 18:18	Story	11/01/23 16:29	RC 70	14/07/23	28/07/23	04/08/23	04/09/23
notifications - intuitive improvements	Highest	To Do	10/01/23 18:22	Story	31/01/23 18:55	RC 72	28/07/23	11/08/23	18/08/23	04/09/23
State Match NCIC Hits	Highest	To Do	10/01/23 18:26	Story	11/01/23 17:46	RC 74	11/08/23	25/08/23	01/09/23	04/09/23
Hotlist NCIC state is not correct	Highest	To Do	09/01/23 20:01	Story	11/01/23 17:46	RC 74	11/08/23	25/08/23	01/09/23	02/10/23
IOS App	Highest	To Do	11/01/23 14:38	Story	11/01/23 16:31	RC 75	25/08/23	08/09/23	15/09/23	02/10/23

Copyright © 2021 Neology, All Rights Reserved.

PAGIS 2843 (update)

- Q&A testing of latest build confirms the following items have been resolved
  - NTP Status Locked flag behavior sometimes not working
  - Hotlist disappearance
  - Hotlist crashing PAGIS
  - Hit delays
  - B/W in overview
  - Random GPS
  - Alert sound is not playing when “Capture Mute” option is enabled
  - Default US Datetime format
  - Delay when closing session was fixed
  - Delay when saving sync settings was fixed
  - Default BOSS sync timing set to 60sec
- Q&A Testing revealed additional items:

Recommendation to extend release date two weeks to 3/13/23

  - Undesirable covert hit behavior in PAGIS, covert hit would display hit info in single pane mode. This initially was flagged as BOSS bug but testing revealed its related to PAGIS
  - Dual screen not showing indication of hit when pop-up is disabled
  - Maximizing icon in PAGIS window not active
  - Add additional sync timer control to differentiate between download and upload timings

Copyright © 2021 Neology, All Rights Reserved.

Q&A Process 2844

- Immediate actions are:
  - Review the unit testing process – in progress (March 15th)
  - Re-implement a peer code review process on the development team – in progress (February 28th)
  - Implement load and stress tests for each release – in progress (March 31th)
    - First Load and Stress test is in progress during this Sprint
  - Review in detail the manual testing process – in progress (April 30th)
  - Review in detail the automatic testing process – in progress (April 30th)
  - Perform a root cause analysis of each error that reaches production - Done
  - Add usability test for every change in UI – Completed (February 15th)

Copyright © 2021 Neology, All Rights Reserved.

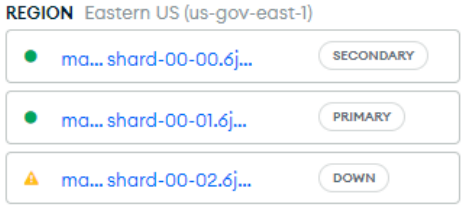
SX4e[2845] Hardware / RMA

- Deep dive analysis on SX4e RMA's is on-going;
- Initial analysis shows no immediate / obvious clustering of same source
  - Dead CMOS Battery; Power Cable Shorted; Win10 Image issues
- Current recommendation is to ensure all units are running latest Software image (at least upgrade from NE220311 to NE220701 image)
- As interim, in addition to Service Spares already provided to MSP, an additional SX4e (with current imaging, extended production soak etc) shall be provided as hot spare to MSP to minimize Mobile Unit downtime.

Copyright © 2021 Neology, All Rights Reserved.

1/24[2846] – Incident Overview - Closed

- Partial Outage of BOSS4 User-Interface with degraded service caused by one (of three) nodes being unresponsive
- Impact was seen on one microservice (API Gateway) linked to User Interface although all other parts of the system continued to function. No additional impact since 1/24.
- Automatic restarts and reconnection is built into this part of the system however continued instability resulted in manual intervention by Neology Tech Support team
- Total length of incident from initial automated activity through to restoration and completion of system health checks was 1hr 41min.
- On-going analysis of log files continues – initial analysis noted Node/Cluster restarts and rebalancing. Involving 3rd line team in analysis
- Suggestion made that where user interruption / outage is noted that Neology is provided with MSP User Email Group so notifications can be sent out to avoid users routing via Noah.
- Actions
  - Today 1/25 The incident will continue to be analyzed by the Solutions Delivery team
  - The case with Mongo will also be escalated because the incident occurred on the database side. Tech support case was created (1081)
  - An improvement in monitoring will be analyzed and implemented to identify this case in a more timely and automatic manner (Feb 10th). In deployment, additional scripts created to manage the log files.
  - The micro-service will be improved so that if the connection to the default node of the database cluster fails, it will try it with the next one (will be released with RC60 in May).



Copyright © 2021 Neology, All Rights Reserved.

2847



Thank you

Copyright © 2021 Neology, All Rights Reserved.



PAGIS User & Administrator Training

Police ALPR Graphical Interface Software

PAGIS Ver. 2.15

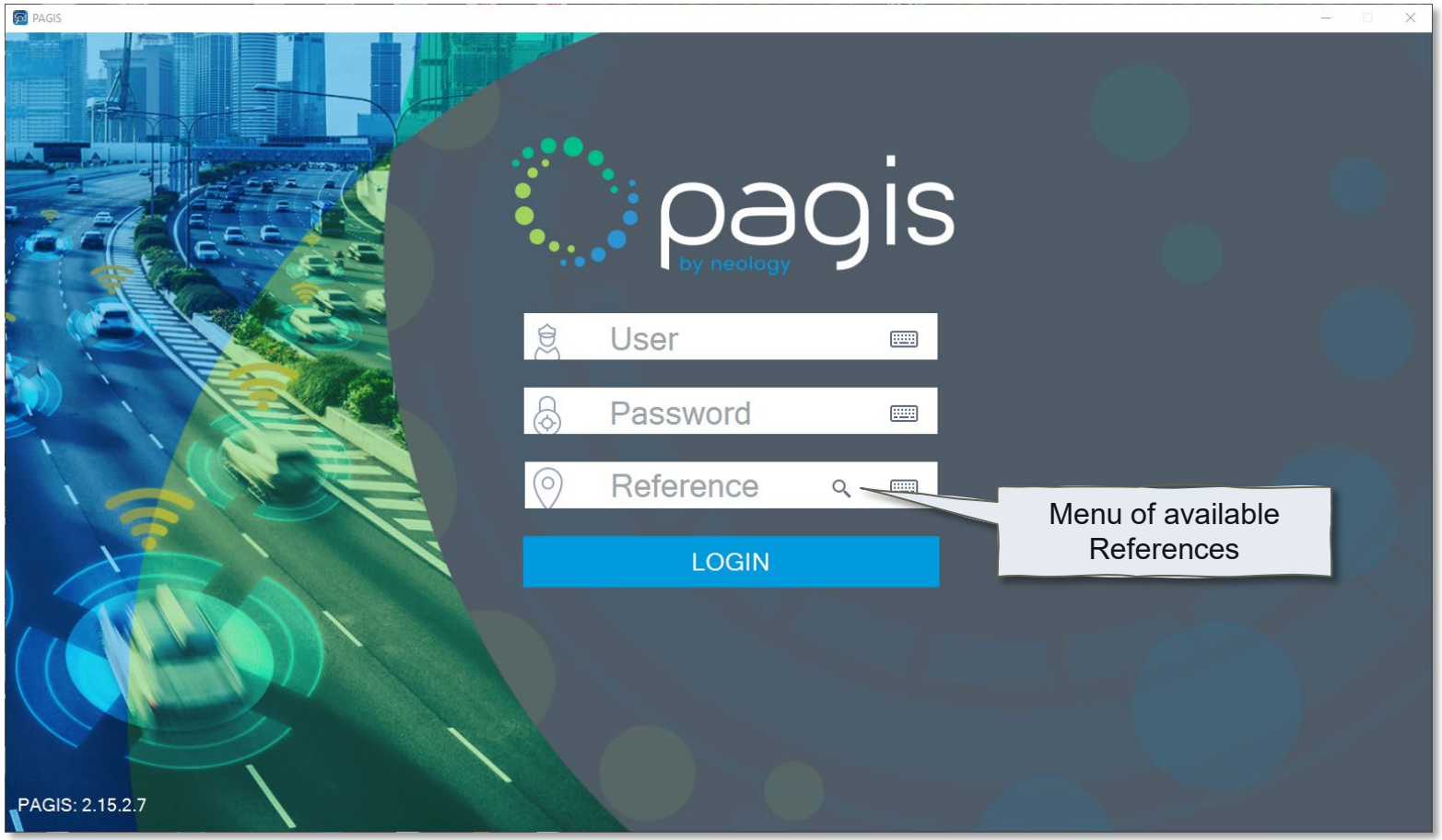
Rev. 06/20/22

Starting PAGIS



To start, double click the **PAGIS** icon on desktop.

- **User-** Enter assigned username.
- **Password-** Enter assigned password.
- **Reference-** Select or Enter department, location or activity specific reference. Each license plate read will have this label associated with it when the field is populated, this field can be used as an additional search filter to sort data in BOSS reports.
- **Keypad-** Available throughout PAGIS where keyboard symbol is present.
- **LOGIN-** Initiate login.



Copyright © 2021 Neology, All Rights Reserved.

Main View Screen

PAGIS System Control Features.

Infrared plate patch
(IR plate Read or “patch”)

OCR text translation of plate patch.

NTP GPS Lock/Unlocked watermark.

Color Overview
Captures are displayed as static images.

GPS Status/Coordinates and Camera Name



Capture panes are blank until camera captures plate.

Copyright © 2021 Neology, All Rights Reserved.

Watermark- About 2851

GPS Locked displayed on images that have confirmed GPS signal.

GPS Not Locked displayed on images that have lost GPS signal.

Watermark stamp is placed on both IR & Color images patch.

Color Patch Watermark Contains:

I. NTP Status: Locked or Not Locked.

II. UTC format: M/DD/YYYY HH:mm:ss.fff.

III. GPS Coordinates Locked or Not Locked.

IV. Computer name of PAGIS client and the mobile processor serial number.

IR Patch Watermark Contains:

I. M/DD/YYYY HH:MM:SS.

II. OCR Plate number & Confidence level.

III. NTP Locked or Not Locked status.

IR patch watermark not shown in live view, only shown in review. See below image.



IR Watermark as seen in review.

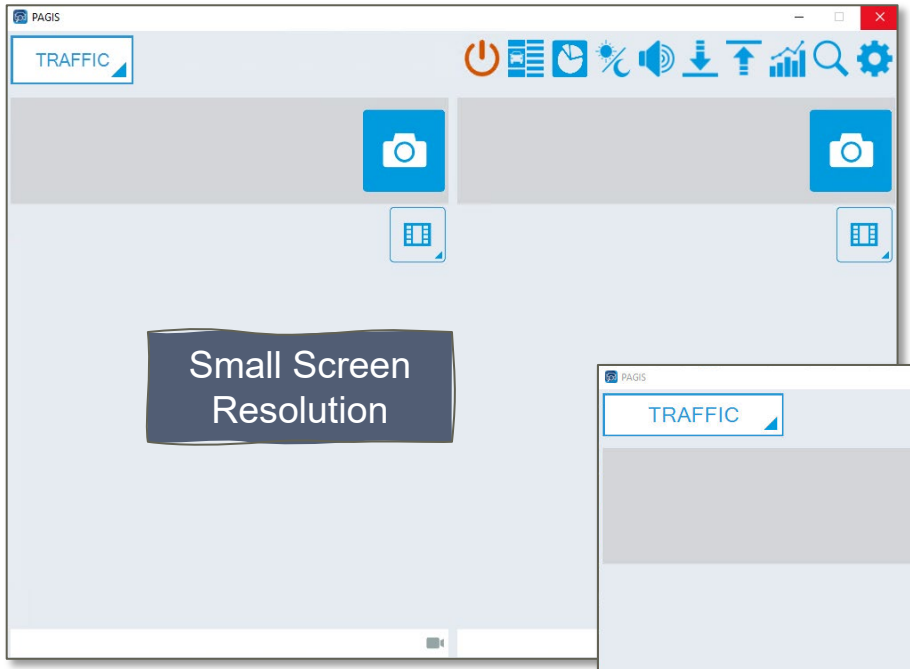


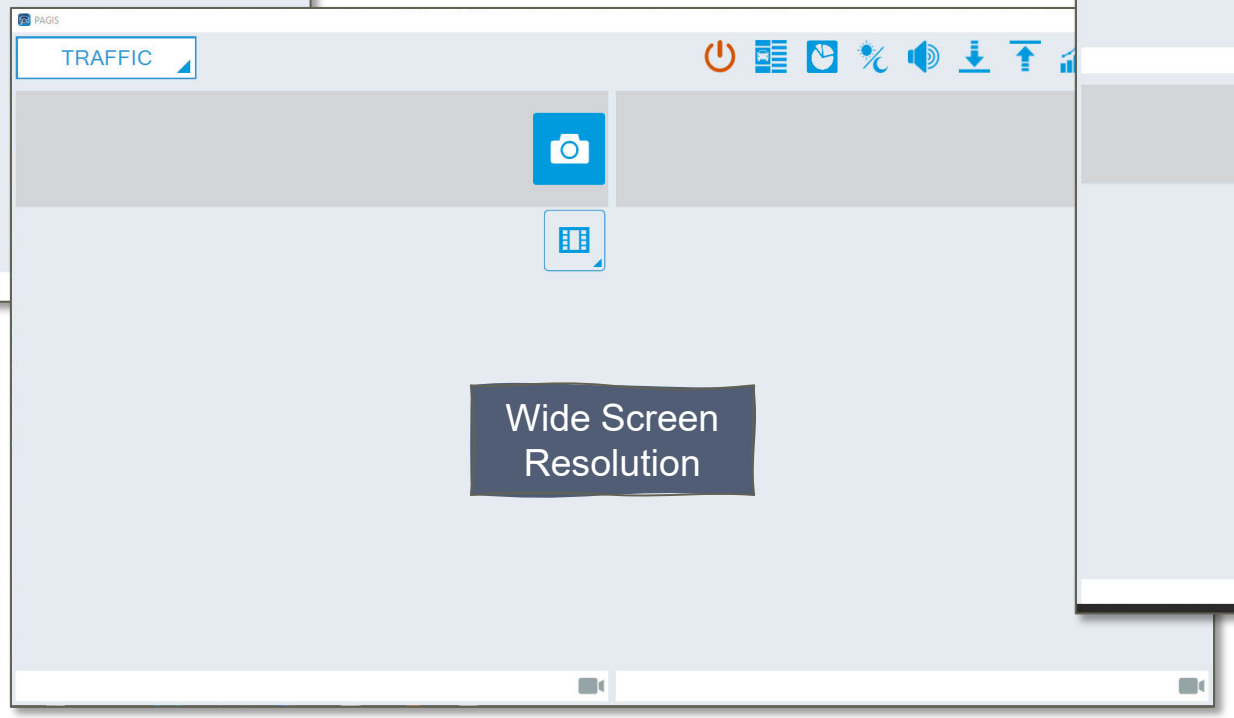
Copyright © 2021 Neology, All Rights Reserved.

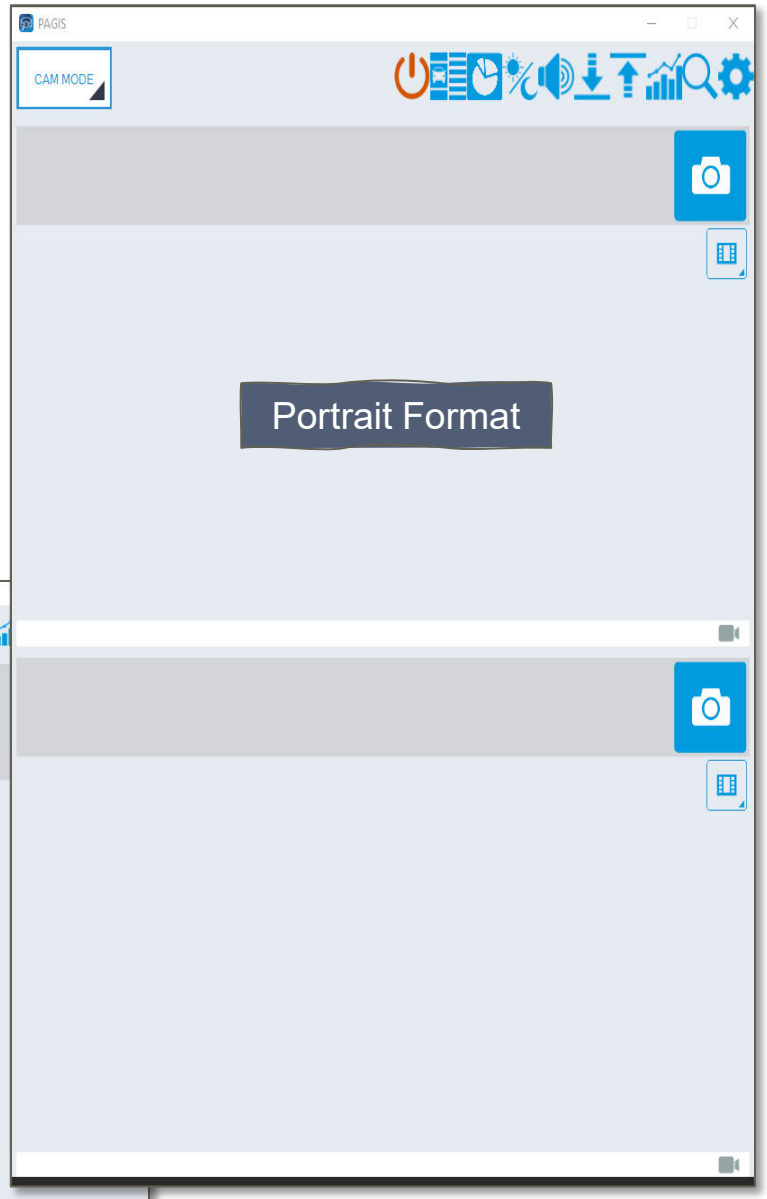
Auto Screen Scaling

2852

PAGIS 2.15 support auto scaling to various screen resolutions and orientations.







Copyright © 2021 Neology, All Rights Reserved.

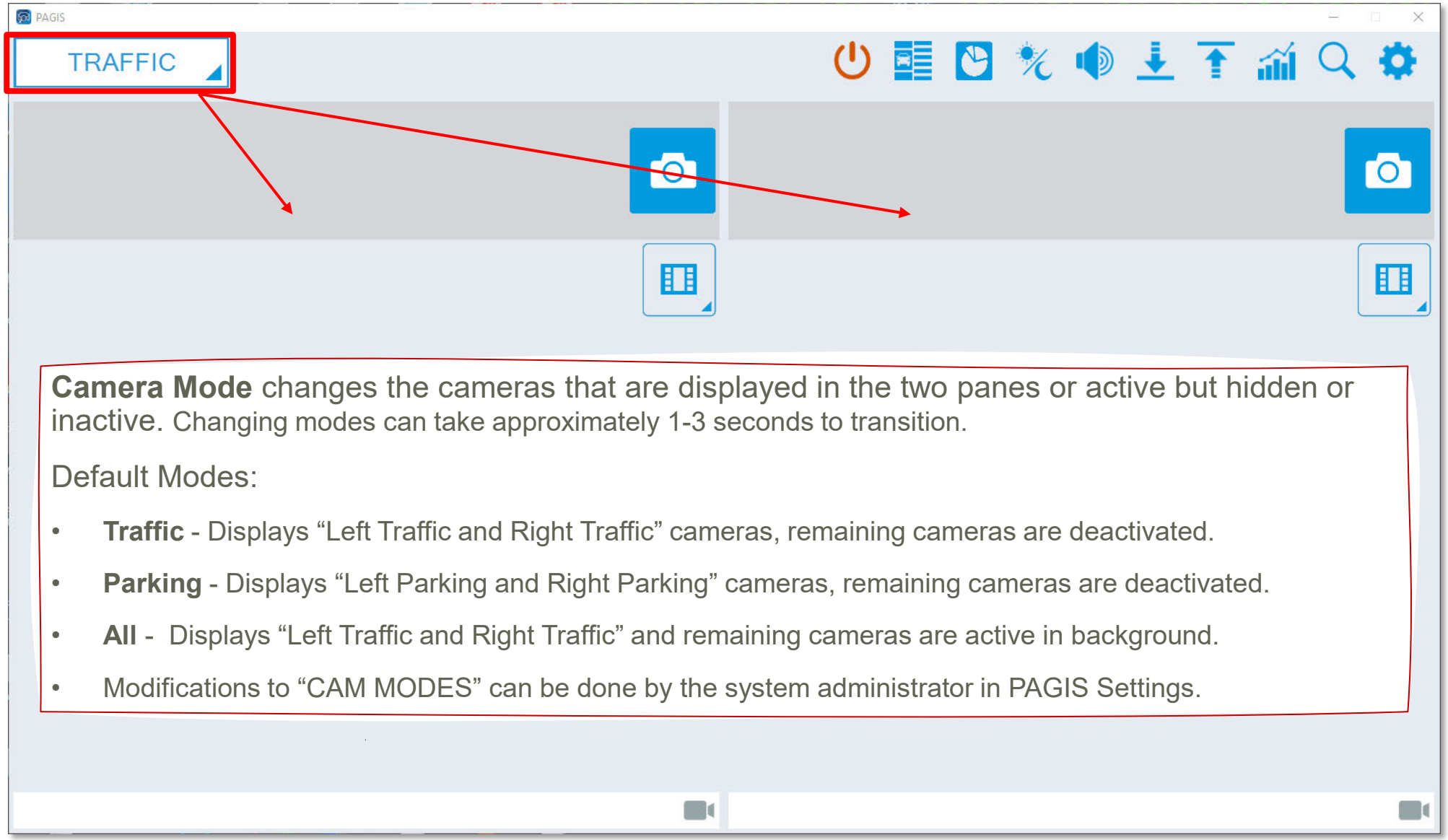
System Controls



	**Logoff button:** When selected, the user will be logged out of PAGIS and return to the login screen. When Auto-login is enabled, this will close PAGIS.
	**Panel Mode:** Switch between Dule or Single panel modes in main live view screen.
	**System Status:** The system status screen provides an area where users can check on the available resources that effect PAGIS performance.
	**Day/Nite mode:** Switch PAGIS between day & night mode screen skins.
	**Sound button**: When selected, this will toggle the PAGIS Read capture sound On or Off, alert sounds will remain active.
	**Begin Shift / Download button:** Performs an BeginShift sequence that downloads Hotlist, Hotplate, Users credentials and targets from the Host. **End Shift / Upload button:** Performs an Endshift sequence that uploads captured Reads, Hits and PAGIS Audit information to the connected Host.
	**Statistics/Review button:** When selected the user can review Alert list, Reads, Hits, Targets, and other PAGIS information.
	**Search button**: Research all available Reads/Hits as well as manually add hotplates to PAGIS's local Hotlist list known as "Manual Reports".
	**Settings button:** Available to Users with administrator rights to modify PAGIS configurations.
	**Firmware & Software update:** This icon will appear when PAGIS detects a new software or camera firmware version is available. All user types are notified, but only Admins can apply the update.

Copyright © 2021 Neology, All Rights Reserved.

Camera Mode – Dule Pane Mode



Camera Mode changes the cameras that are displayed in the two panes or active but hidden or inactive. Changing modes can take approximately 1-3 seconds to transition.

Default Modes:

- **Traffic** - Displays “Left Traffic and Right Traffic” cameras, remaining cameras are deactivated.
- **Parking** - Displays “Left Parking and Right Parking” cameras, remaining cameras are deactivated.
- **All** - Displays “Left Traffic and Right Traffic” and remaining cameras are active in background.
- Modifications to “CAM MODES” can be done by the system administrator in PAGIS Settings.

Copyright © 2021 Neology, All Rights Reserved.

2855 Camera Panel Controls

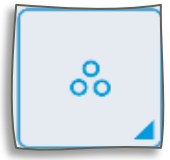




Take Pic: Just above the Camera View Selector button is “Take Pic”. This button allows the user to quickly take a picture from the camera in the current view.



Static View: This is the default state at login showing the Static View of captured events.
(NOTE: PAGIS does not automatically display a live feed.)



Color View: Clicking the Camera View selector button once, will switch to the Color feed. This displays the current live view of the color camera and will time out after 60 seconds or until the next capture event, which ever occurs first.



IR View: Clicking the Camera View Selector button twice, will switch to the Infrared (IR) feed. This displays the current live view of the IR camera and will time out after 60 seconds or until the next capture event, which ever occurs first.

Copyright © 2021 Neology, All Rights Reserved.

Take Picture

2856

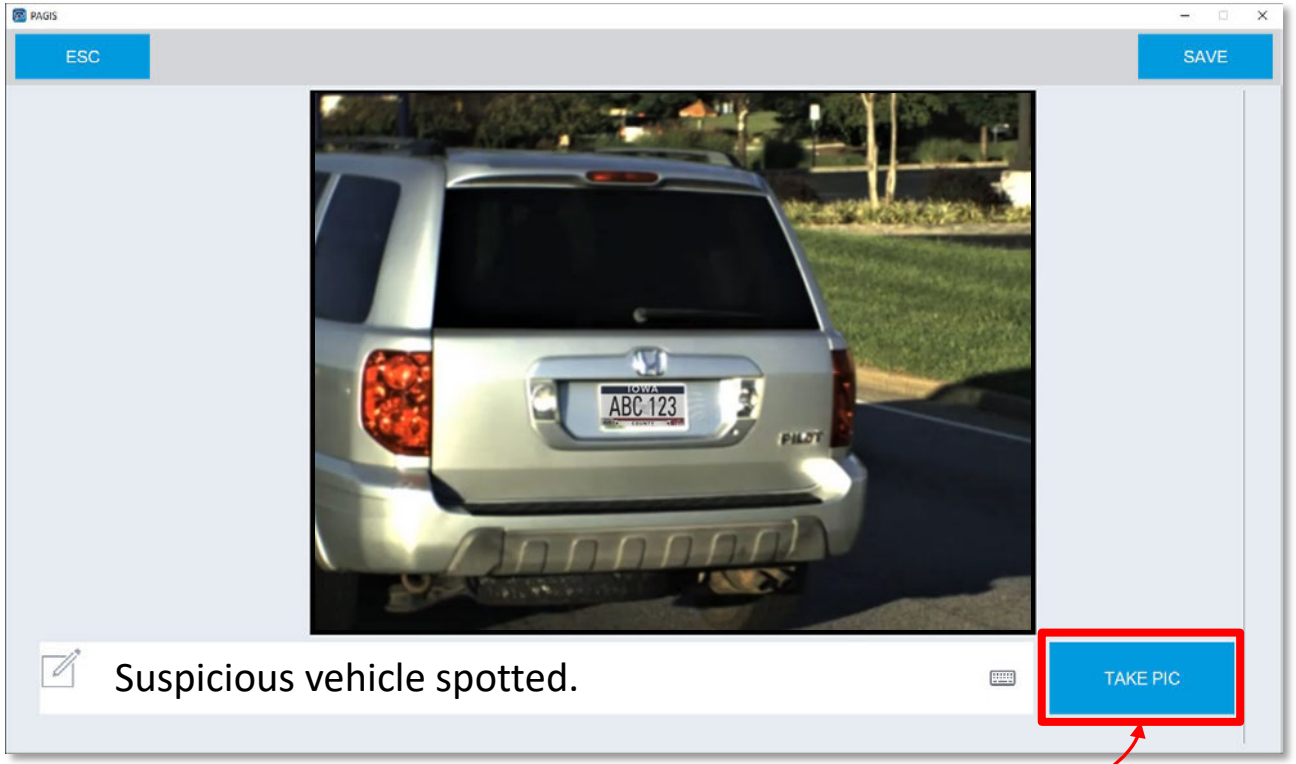
Take a Picture:

- From the Main View Screen, press the Take Pic button from the desired camera.
- The image taken will be displayed.
- Enter a description of the picture in the text field at the bottom of the screen.
- To save picture click the SAVE button, ESC to cancel. Either action will return you to Main View Screen.

NOTE: The picture will not save if a description is not entered into the text box.

View Saved Images:

- Navigate to the Review menu in PAGIS.
- Select Audits.
- The user will be able to see a thumbnail of the image and the saved notes.
- In order to review the saved images after purge, the user will need to run the Audit Image Report from BOSS.



Toggle “Take Pic” button to activate live and capture mode.

Copyright © 2021 Neology, All Rights Reserved.

Camera Mode – Single Pane Mode

Single Pane: The single pane displays has one large active capture area on the left of the screen, this area will display all current captures in real-time. The panel on the right show you past captures, updates populate from the top down.

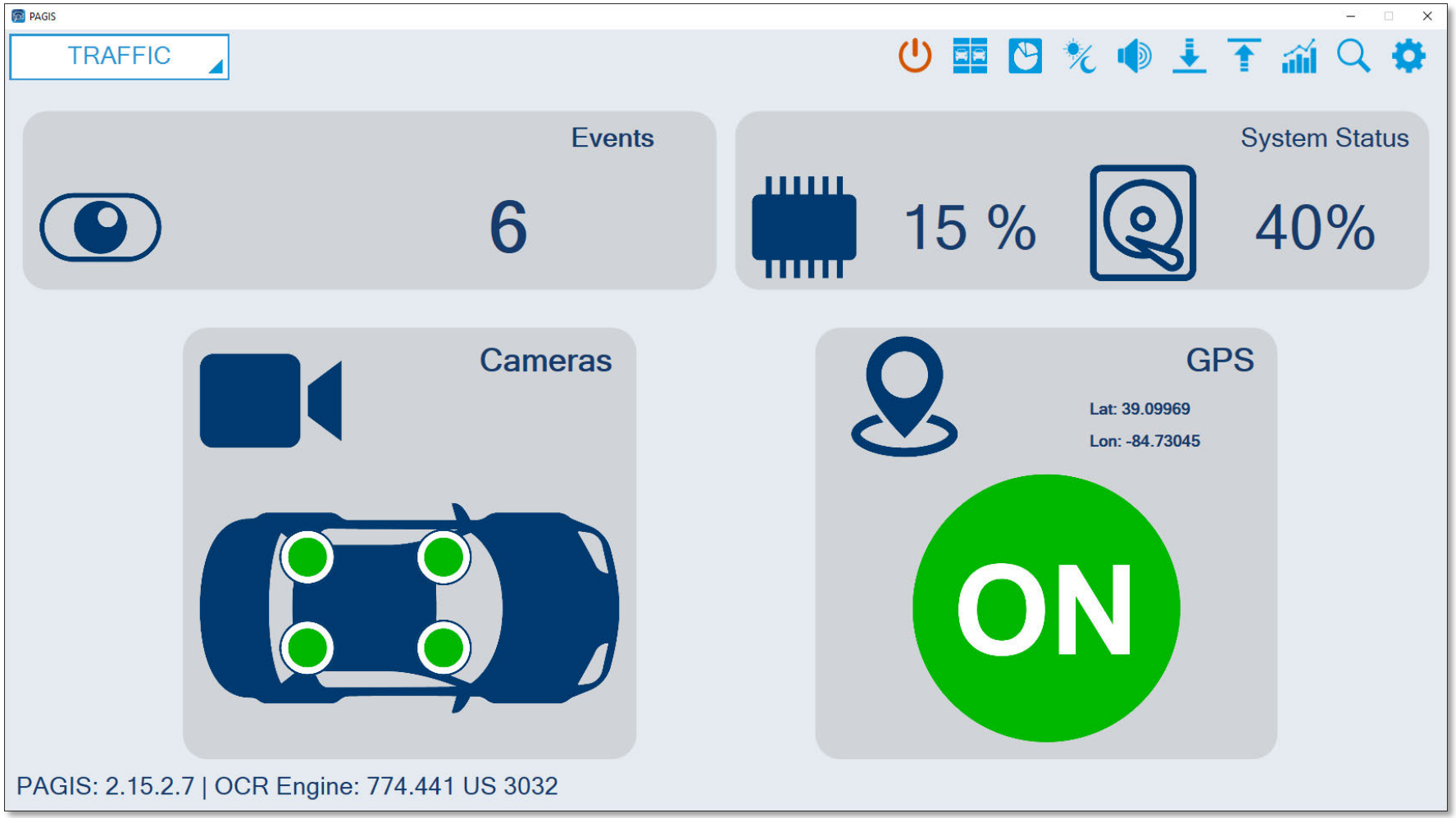
- **Cam Mode:** Controls which cameras are active in the main display.
- **Last / Live:** Set the active capturer panel to static or live view. The Live mode alters the panel arrangement slightly, showing only two primary cameras on the left w/ no image patches.
- **All Reads / Hits:** Toggles to show only hits or reads in the history panel.



Copyright © 2021 Neology, All Rights Reserved.

PAGIS Status View





Status View

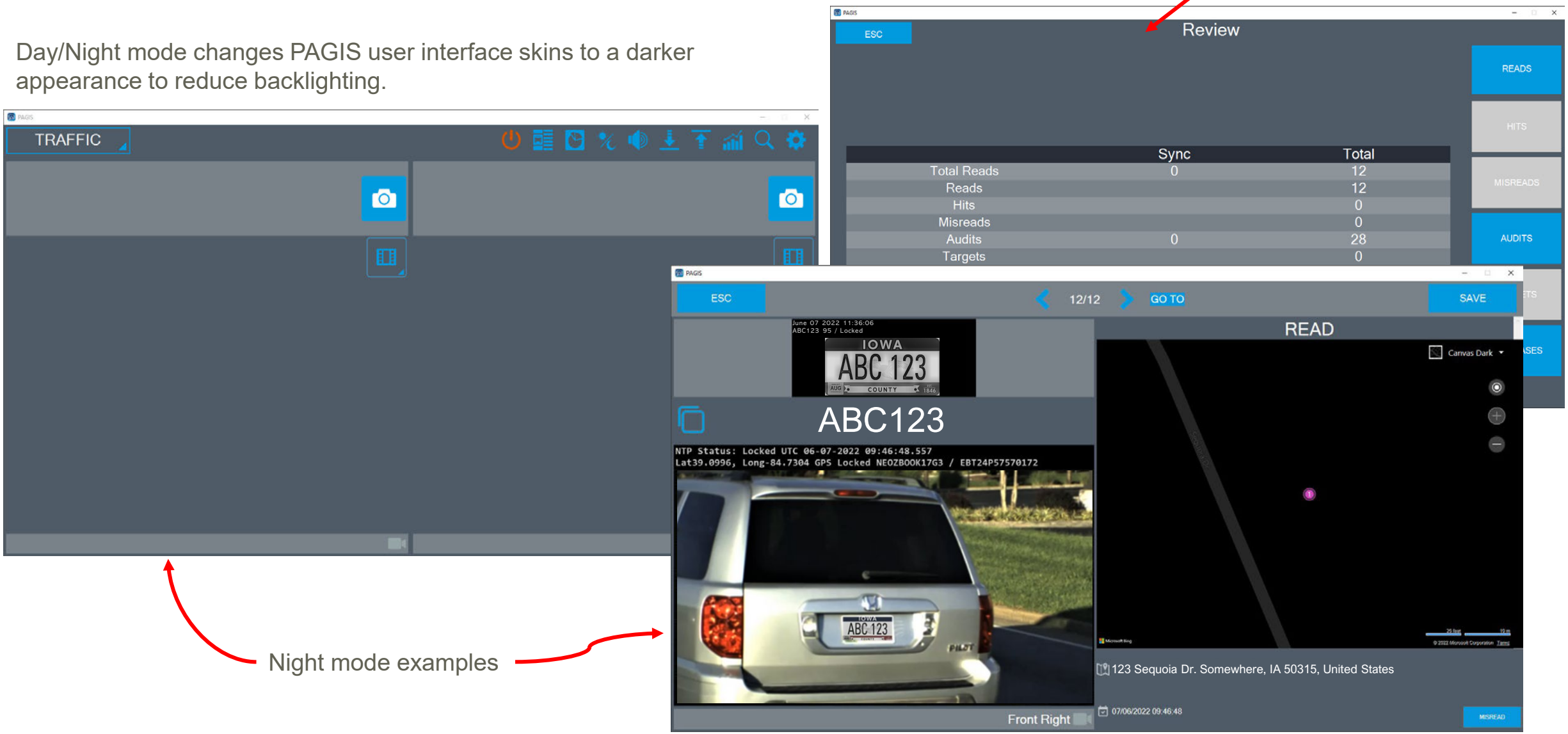
The status panel provides a means of monitoring key system resources important to PAGIS operations.

- **Events-** The events show the current number of captured plates in PAGIS.
- **System Status-** Displays the amount of RAM & DISK usage of the computer PAGIS is running on.
- **Cameras-** This indicates which cameras are active from the selected “CAM MODE”.
- **GPS-** Displays if PAGIS currently has an active GPS signal.
- PAGIS and OCR Engine versions shown in bottom left.

Copyright © 2021 Neology, All Rights Reserved.

Night Mode Screens

Day/Night mode changes PAGIS user interface skins to a darker appearance to reduce backlighting.



Night mode examples

Copyright © 2021 Neology, All Rights Reserved.

Data Synchronization

2860

Data synchronization can be configured one of three ways depending on usage type. Its important to understand which option PAGIS is configured, as they dictate different user interaction.

USB Sync- This method of synchronization requires that the PAGIS user manually activate the upload/download button to send/retrieve data from an external USB drive.

Boss Sync without Purge- When “Boss-Sync” is enabled all data will be automatically synchronization between PAGIS and BOSS, this included Users, Alert-List, Reads/Hits & Audit data. The exception in this option is that locally stored data remains accessible in PAGIS, this includes Reads/Hits & Manual Reports entries, they will remain local until the Upload button is activated upon which those data sets will be purged from PAGIS.

Boss Sync with Purge- When “Boss-Sync” is enabled all data will be automatically synchronization between PAGIS and BOSS, this included Users, Alert-List, Reads/Hits and Audit data. With the Purge setting enabled it is not necessary for the PAGIS user to manually activate the Upload button to purge locally stored data as this will be maintained by PAGIS based on purge Privacy settings configured, purging occurs each time PAGIS is started.



Typ. Download Status Messages

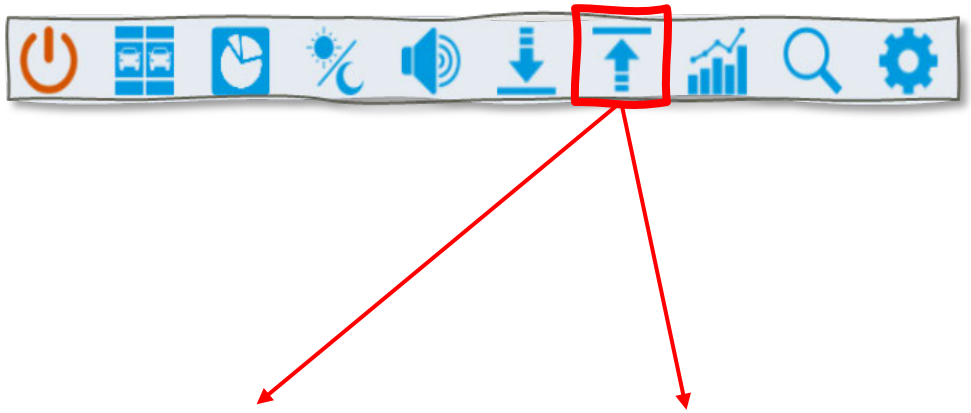
- Performing beginshift synchronization...
- Session started, checking for updates!
- Retrieving plates for COUNTY WARRANTS

Typ. Upload Status Messages

- Exporting endshift read data at event 0 of 28...
- Purging audit data. This may take a while, please do not power off!
- Endshift synchronization succeeded!

Copyright © 2021 Neology, All Rights Reserved.

First Time PAGIS Activation 2861



Newly activated mobile devices must be enabled and configured at the BOSS software once the primary host IP has been entered and saved into PAGIS.

- Activating the download button will manually initiate communication with BOSS, during this process the user will see sync status messages. First time synchronization BOSS will acknowledge the communication with a rejection message titled “HttpStatusCode Unauthorized” signifying BOSS has seen the request, created the device listing but rejected the communicated pending user activation in BOSS.
- The PAGIS auto sync feature will also attempt communication with BOSS on a reoccurring cycle, about once every 10-20 seconds, the device listing will still appear in BOSS, but the PAGIS user will not see any dialog box’s indicating the status.

BOSS acknowledgement and rejection message	Failure to communicate with BOSS message
Performing beginshift synchronization...	Performing beginshift synchronization...
Error Synchronizing Data. Please check log for more information.	Error Synchronizing Data. Please check log for more information.
HttpStatusCode Unauthorized; unable to get data	Error syncing data with BOSS. Please check wireless connection and try again.

Copyright © 2021 Neology, All Rights Reserved.

Review Section



Reads- Review all plate detections that have occurred since the last upload or data purge cycle.

Hits- Review Hit alerts that occurred since the last upload or data purge cycle.

Misreads- Review Reads that have been manually flagged during the shift as misreads.

Audits- Review failed and successful login's, any manual data entered during the shift, pictures taken and all manual license plate searches.

Targets- Review targets that have been synchronized from Boss.

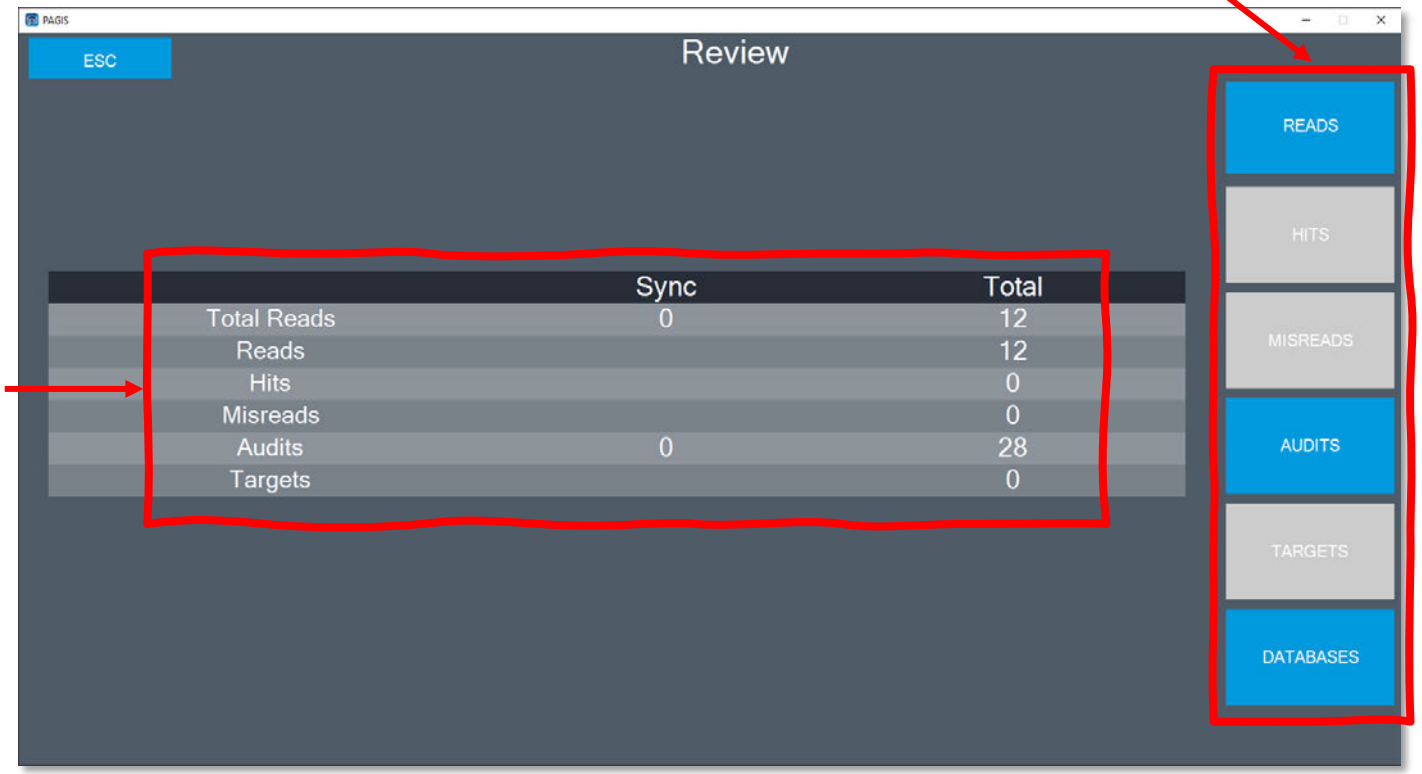
Databases- Review the all the databases currently in PAGIS.



Click Review from the Main View screen to display additional options for reviewing data.

- **Total Reads-** Shows the total number of Reads/Hits collected and the amount synced.
- **Reads-** Shows only the total number of collected Reads.
- **Hits-** Shows only the total number of collected Hits.
- **Misreads-** Shows only the total number of Reads marked as misreads.
- **Audits-** Shows the total number of collected Audits and the number that have synced with BOSS.
- **Targets-** Shows only the number of targets downloaded, they do not sync as they originated from the Boss application.

Note: When PAGIS is setup for Disk-Sync the "Sync" column dose not apply.



Copyright © 2021 Neology, All Rights Reserved.

Review - Reads 2863

Save changes or Esc to return to Main View.
(Typ. thought out review screens)

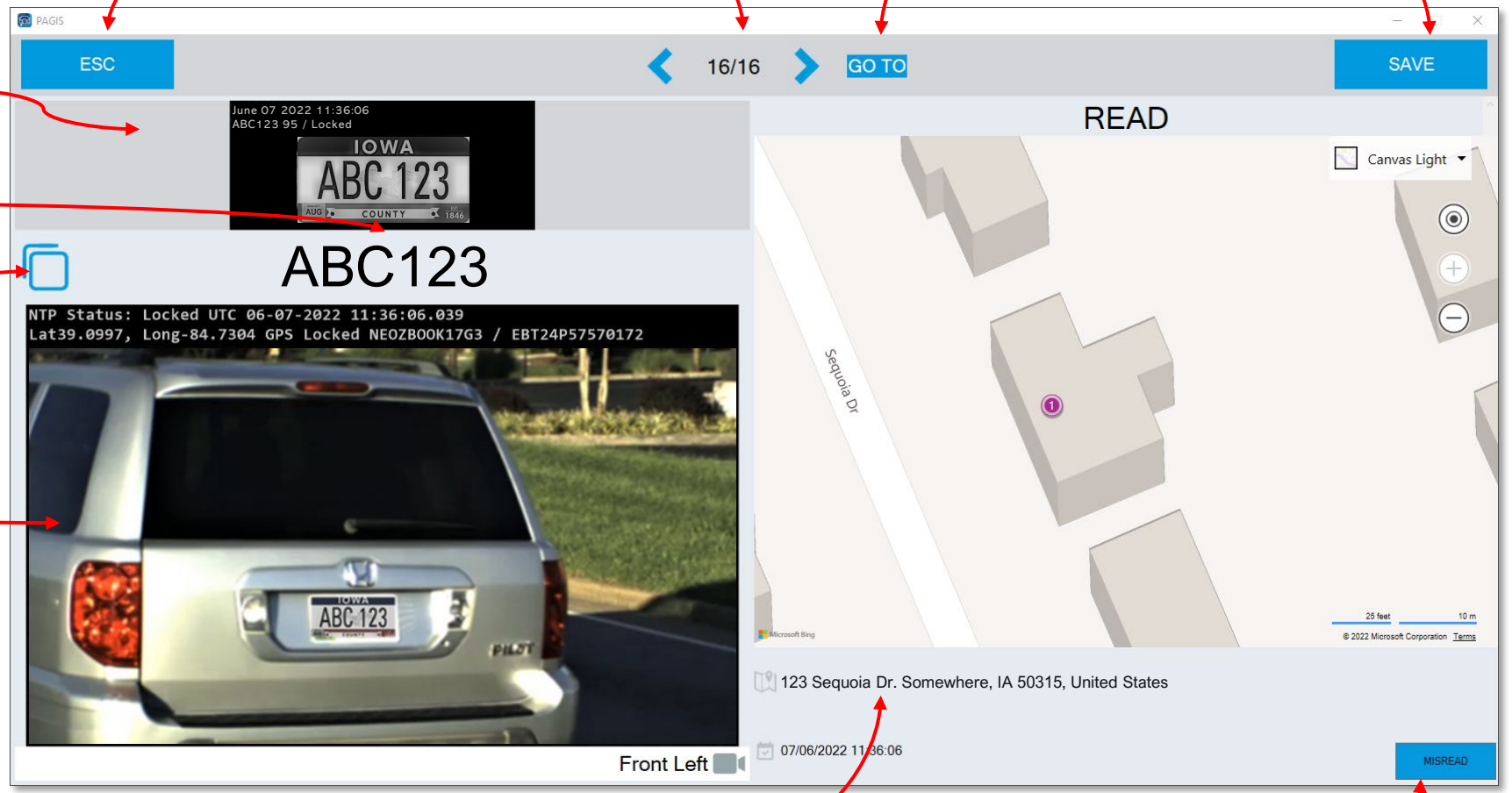
Current view / Total Reads.
Prev. & Next

Jump to specific read.

IR “Plate Patch” w/ NTP watermark
Clicking Plate Patch will result in larger view Of image.

OCR translation of “Plate Patch”
Click OCR Patch to correct a misread.

Copy plate number to clipboard



Color Camera “Overview” *w/ NTP status watermark.*
Clicking overview Patch will result in larger view of image.

Active Mapping with address translation.

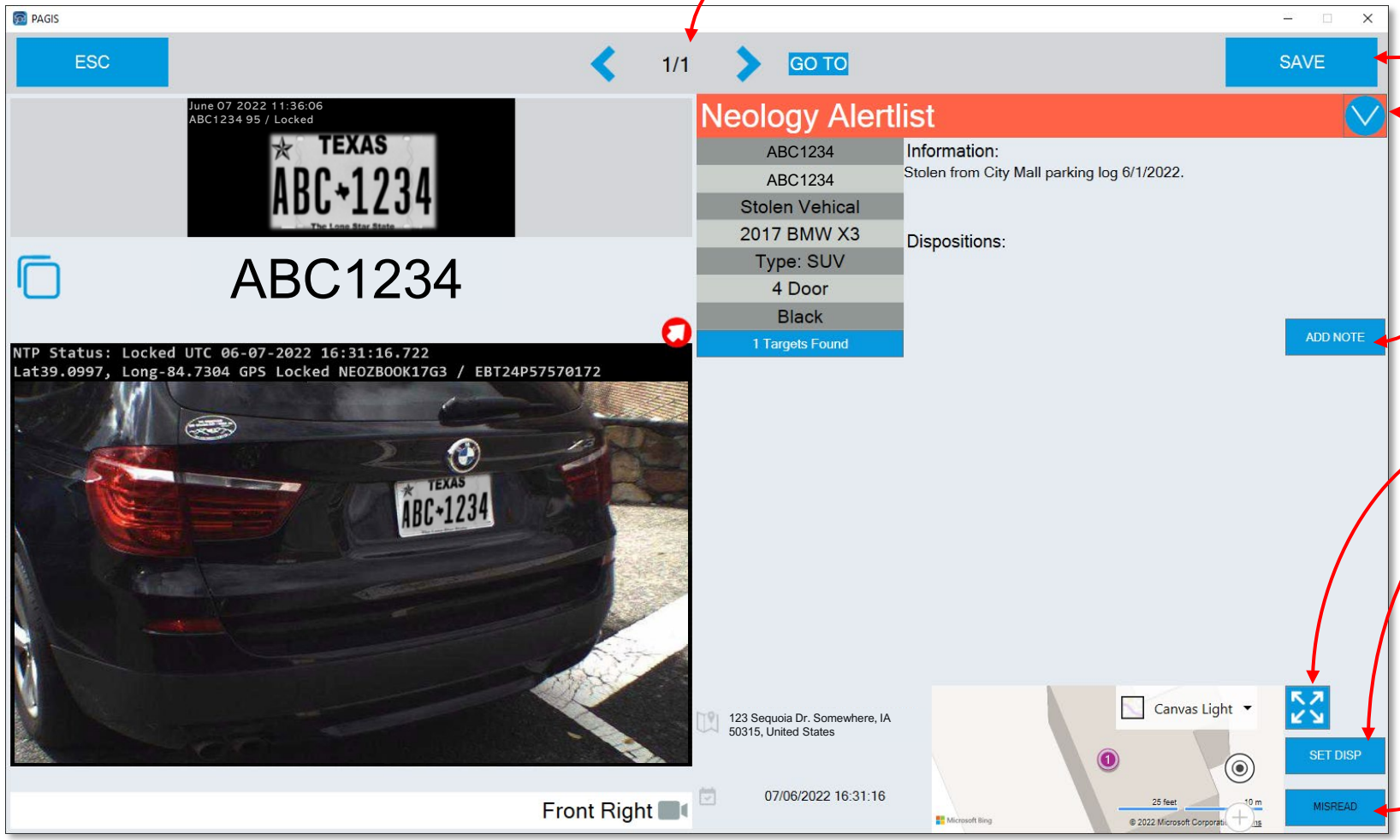
Jump –Move to a specific record.

Copyright © 2021 Neology, All Rights Reserved.

Review - Hits

2864

The **Current / Total** indicates which HIT out of all totals you are reviewing, clicking the arrows on the left or right will let you flip between other registered HITS.



SAVE changes made to notes, dispositions or misread corrections.

Hide/Show hit information.

ADD NOTES – Add information about a particular Hit prior to synchronization to BOSS. For instance, you might add information about the arrest or violation.

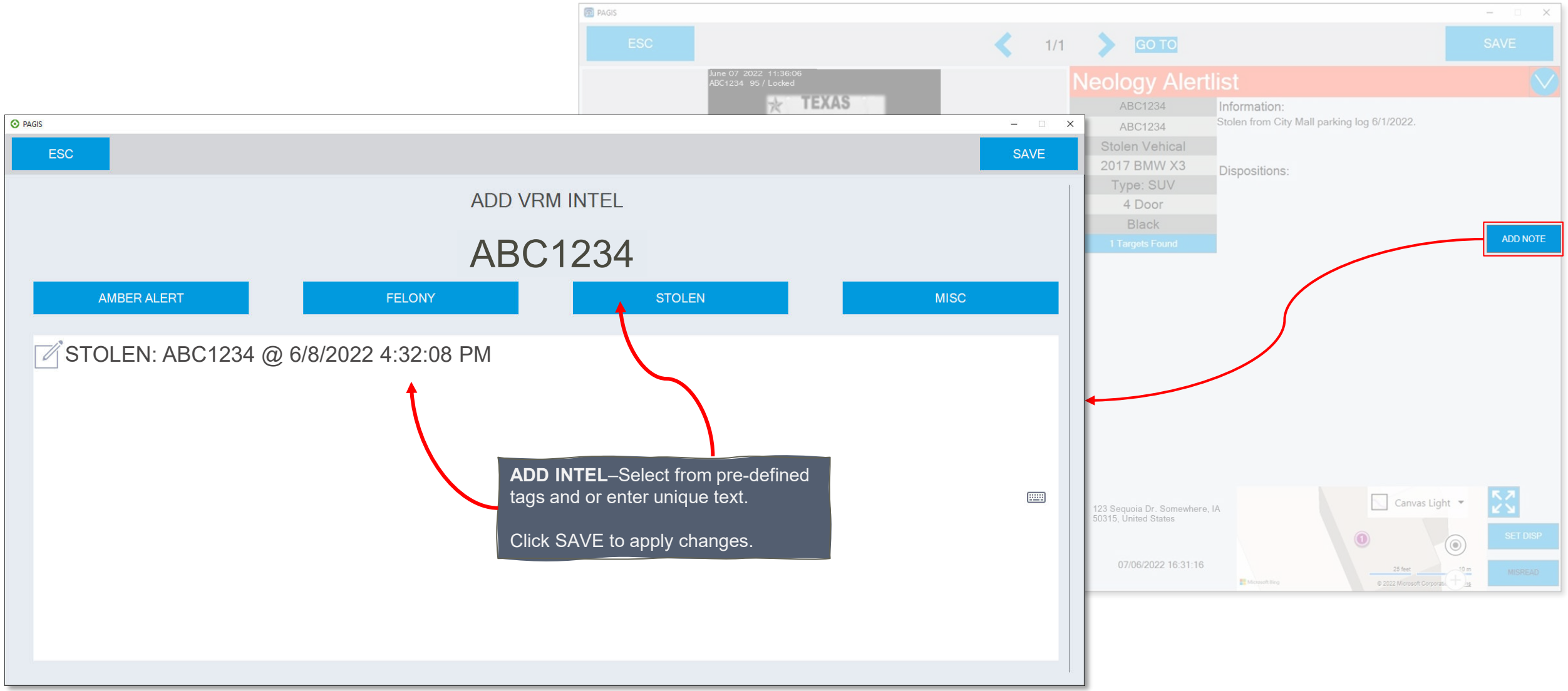
Expand MAP

SET DISP –Report the disposition of a Hit in one of the categories defined by your Boss system administrator, *(Arrest Made, Vehicle Recovered, Surveillance Established, Towed, etc.)*. Dispositions appear in sperate selection window, these dispositions are reported to BOSS and allow for more detailed classification when running a Hit reports.

MISREAD– Add information about a particular Hit prior to synchronization to BOSS. For instance, you might add information about the arrest or violation.

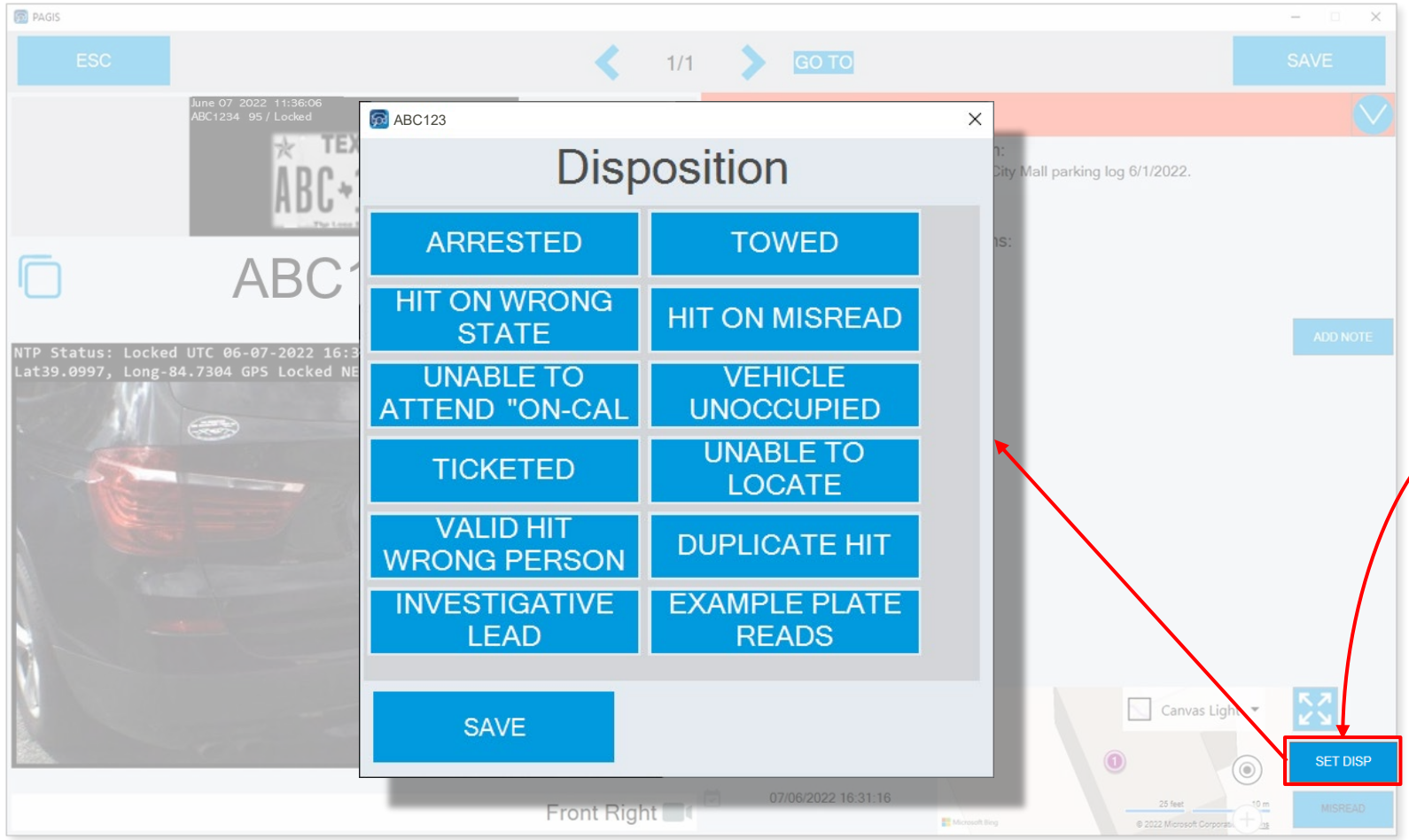
Copyright © 2021 Neology, All Rights Reserved.

2865 Review- Hits- Add Notes



Copyright © 2021 Neology, All Rights Reserved.

2866 Review- Hits- Disposition

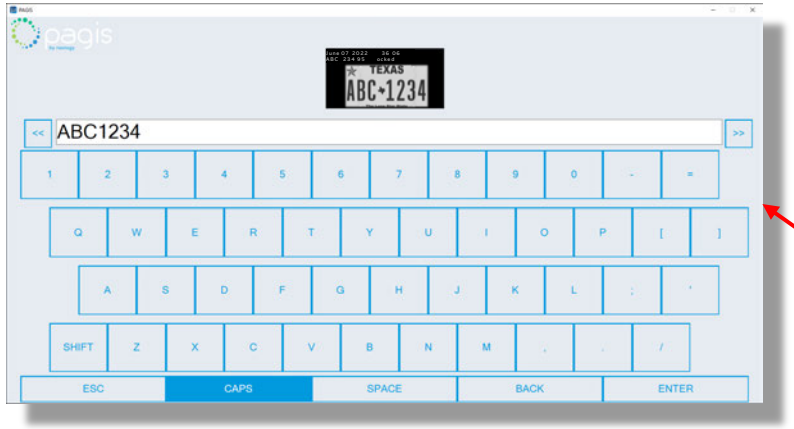


Set Disp –Report on the disposition of the Hit from the deployed categories.
Note: Dispositions are managed by BOSS, additions or edits must be done by system admins.

- Select **One** or **Multiple**.
- **SAVE** to apply selection.

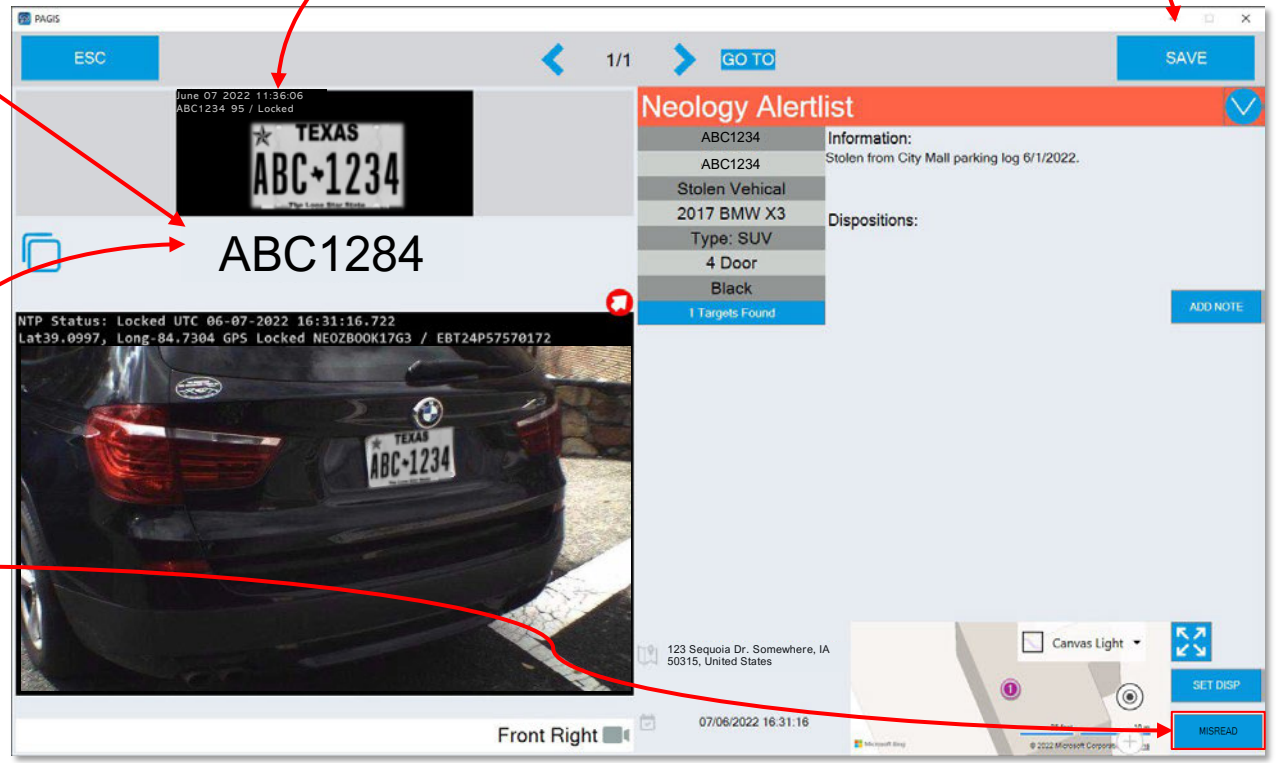
Copyright © 2021 Neology, All Rights Reserved.

2867 Review- Hits/Reads- Misread Correction



"Misread Plate"

Save changes



Correct or tag Read/Hit that have been misread.

- *Click OCR Patch to manually correct a misread, "ENTER" to save.*
- *Click* MISREAD *button to instantly tag event as "Misread" without editing plate number "SAVE" to apply changes.*
- *Hits tagged as misread are demoted to Read and no longer counted as Hit.*

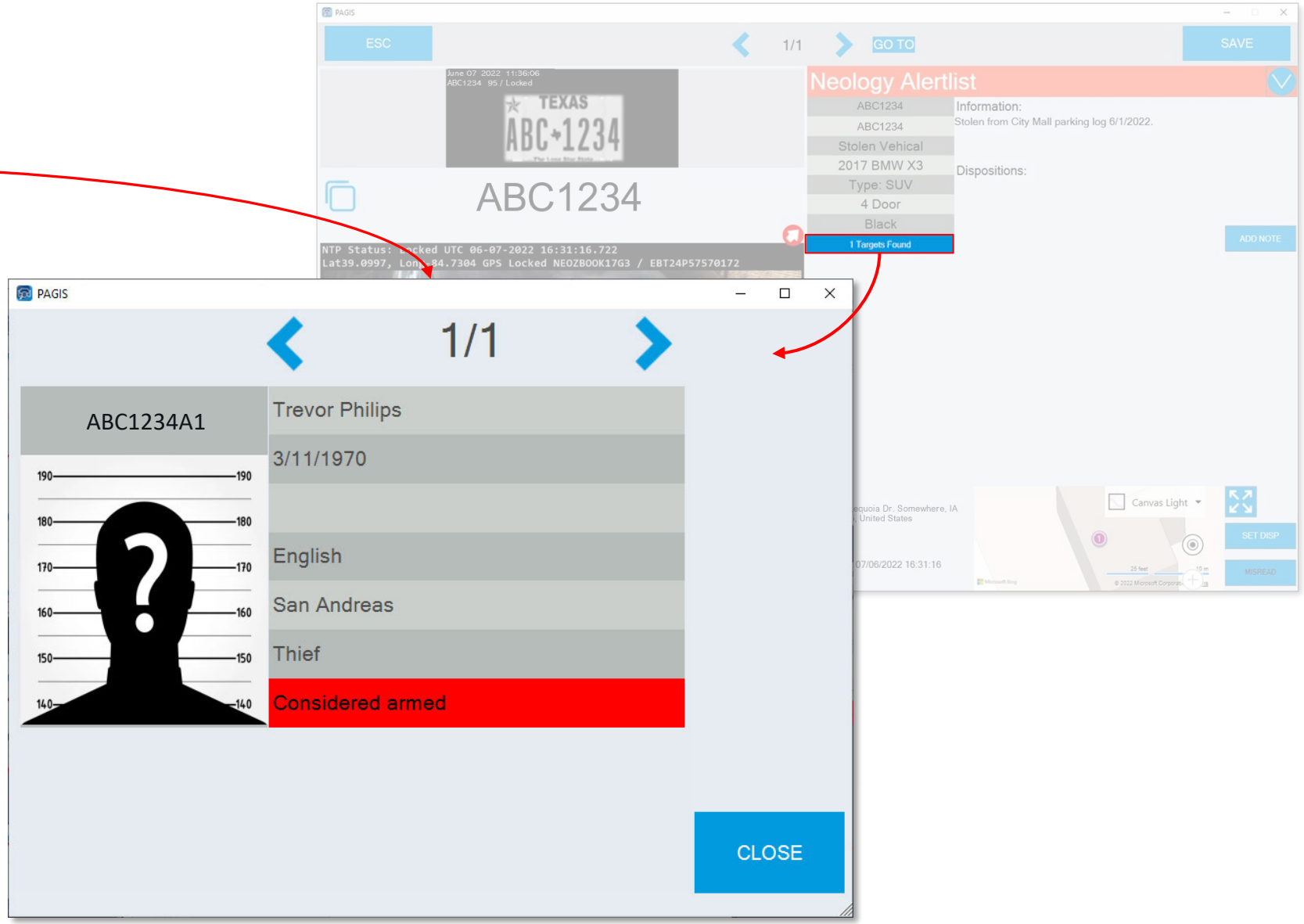
Copyright © 2021 Neology, All Rights Reserved.

Review- Hits-Targets 2868

- **Target Profile**–Target screen displays information about suspects matched with a license plates. Targets are downloaded into PAGIS from the Back Office System Software (BOSS).

- < 1/2 > Click left or right arrows to view additional targets associated with this hit. Number to left is current view, number to right is total targets available.

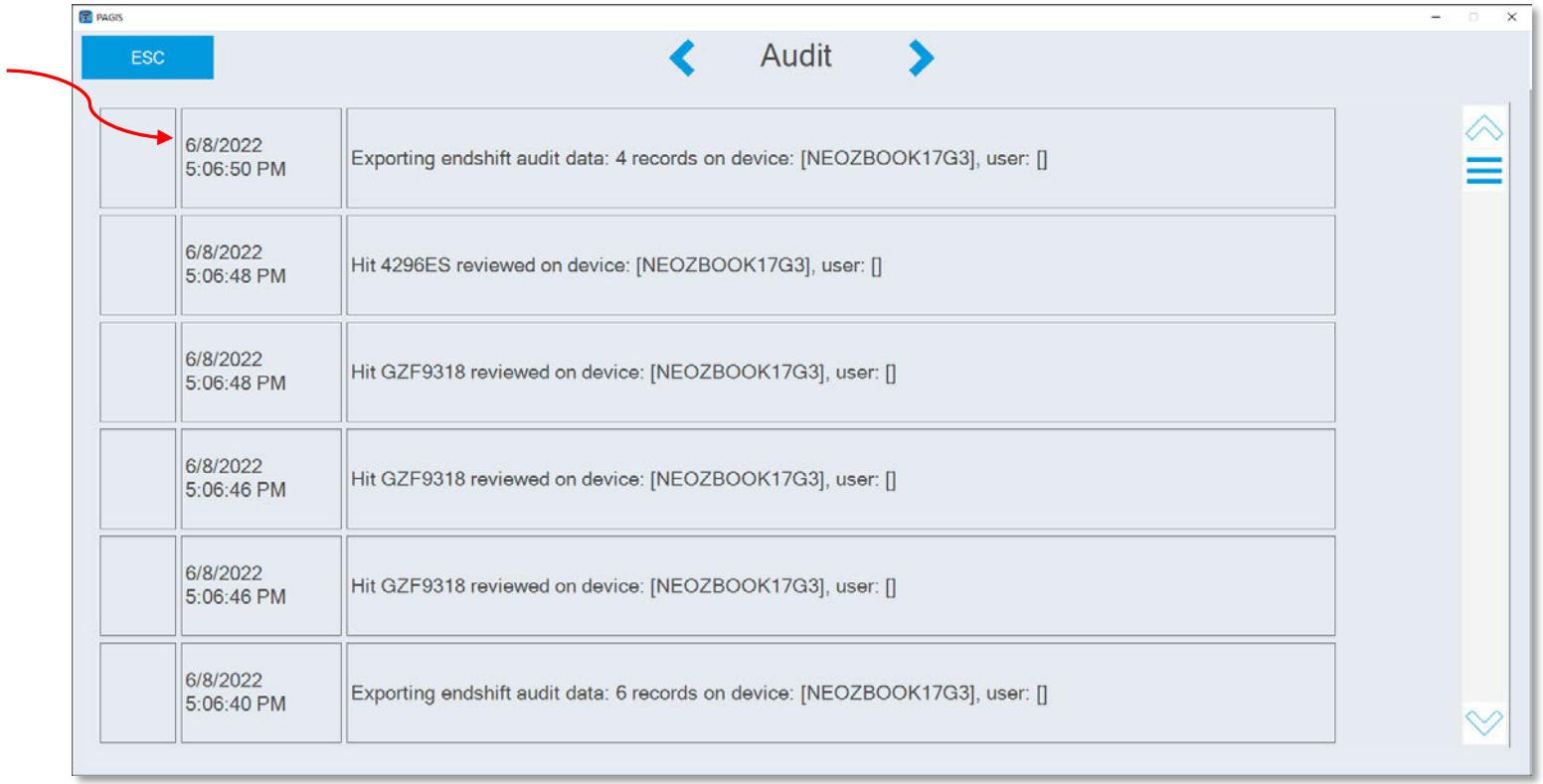
- **Close** – Returns to previous screen.



Copyright © 2021 Neology, All Rights Reserved.

2869 Review- Audits

- The Audits screen provides a log of various actions taken during the current PAGIS session, including searches, synchronizations, Hits, etc. The Audit logs are transmitted back to BOSS during PAGIS Auto-Sync or during a manual Upload cycles. The Audit trail is reset during Upload or Auto purge cycle.
- **Esc-** Return to previous screen.
- **< >-** Cycle thought all available audit log by page, left arrow is previous, right arrow is next.
- **Scroll-** Scroll up/down thought all available Audits.



Copyright © 2021 Neology, All Rights Reserved.

2870 Review- Databases 1 of 2

Database Name – Displays the name and color code of the Alert List, along with Date\Time showing the last synchronization update.

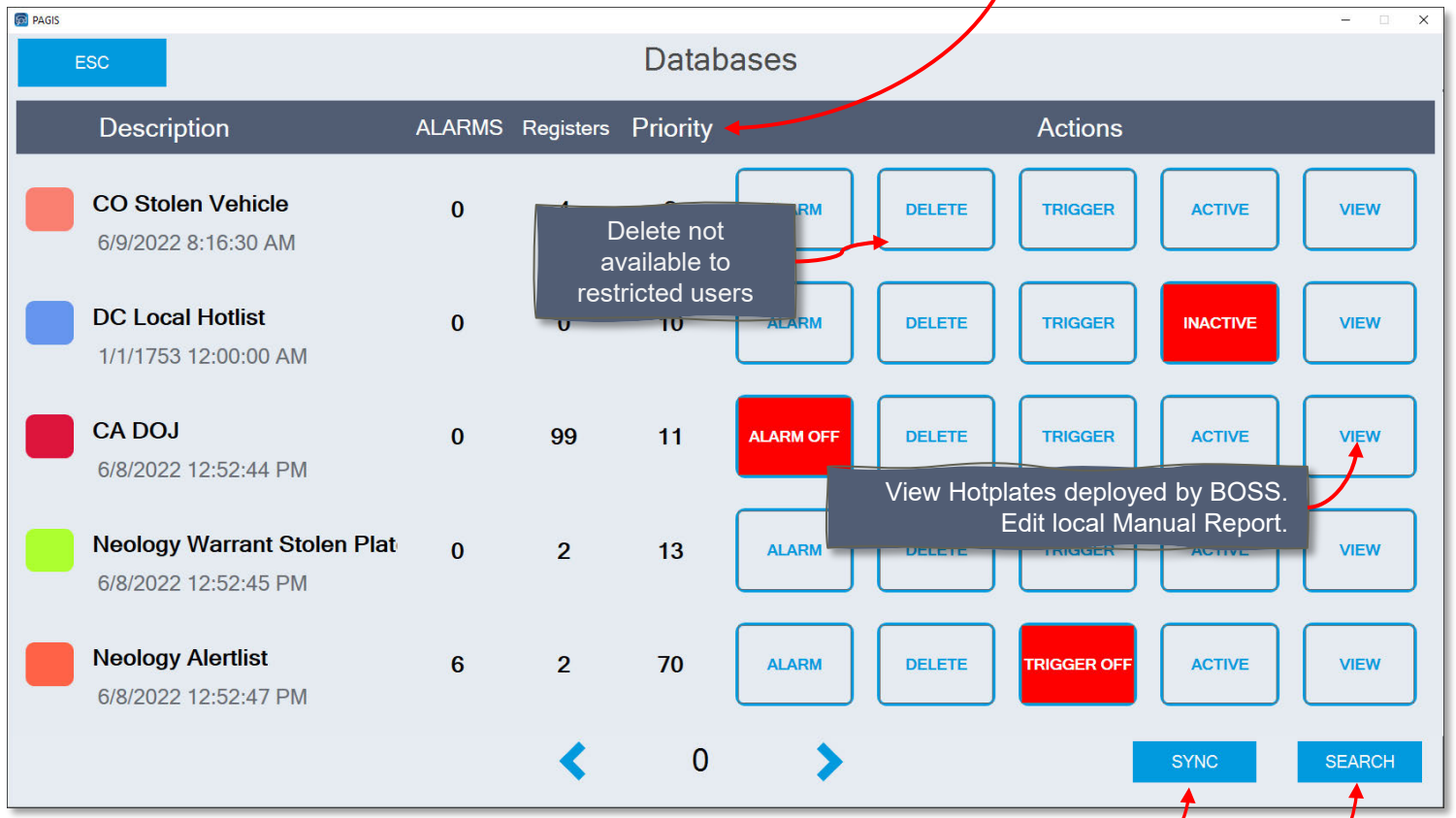
Alarm / Alarm Off- When this button is clicked it will switch from “Alarm” or to “Alarm off” depending on its previous state. “Alarm” means the PAGIS user will be alerted if a Hit occurs. If “Alarm off” is displayed the PAGIS user will not be notified of alert, but the alert will still register.

Delete – Removes the Hotlist from the current session. Because some databases may be managed in BOSS, if deleted and has not been removed from the BOSS deployment list, it will be added back on the next synchronization via Auto-Sync or during the next Download cycle.

Trigger / Trigger Off– If Trigger is on, the software sends a signal to a data com port on the mobile processor and any device (such as a light or siren) connected through this port will active the device during an alert.

Active / Inactive– Database status indicator. A red button shows that the Alert List is inactive, and Hits will not be generated from that Alert List in PAGIS.

Priority – Database priority provides PAGIS a means of displaying Hits with higher priority first if multiple Hits occurs from a single event. Values can be (1-999) as determined by BOSS System Administrator. The lower the number, the higher the Alert List priority. By default, the “Manual Reports” Alert List created by PAGIS has a priority of 500.

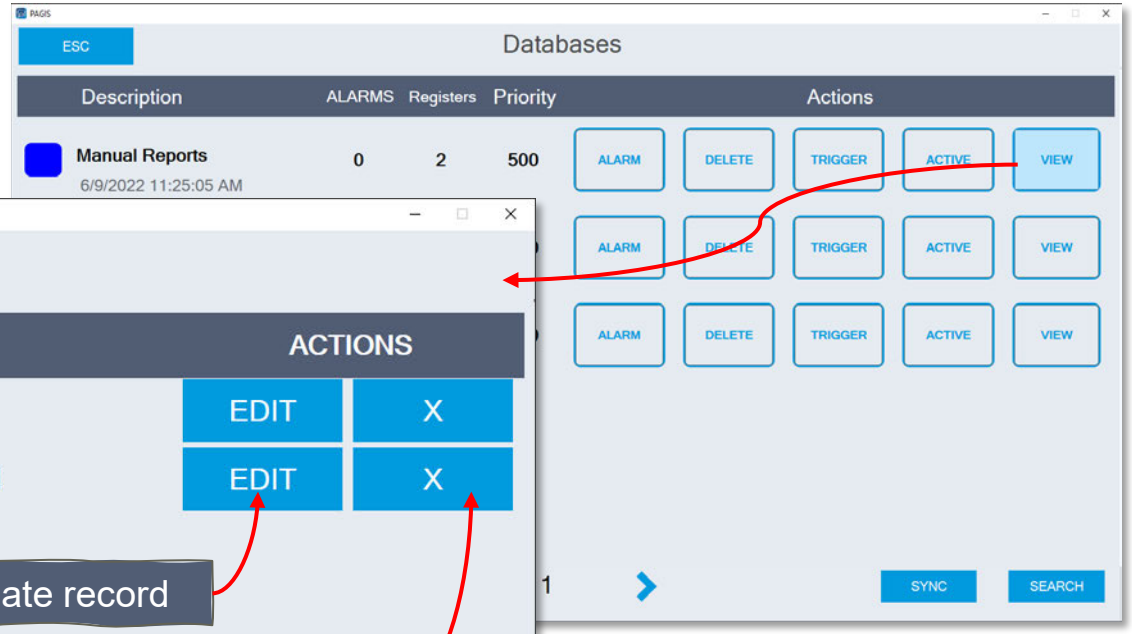


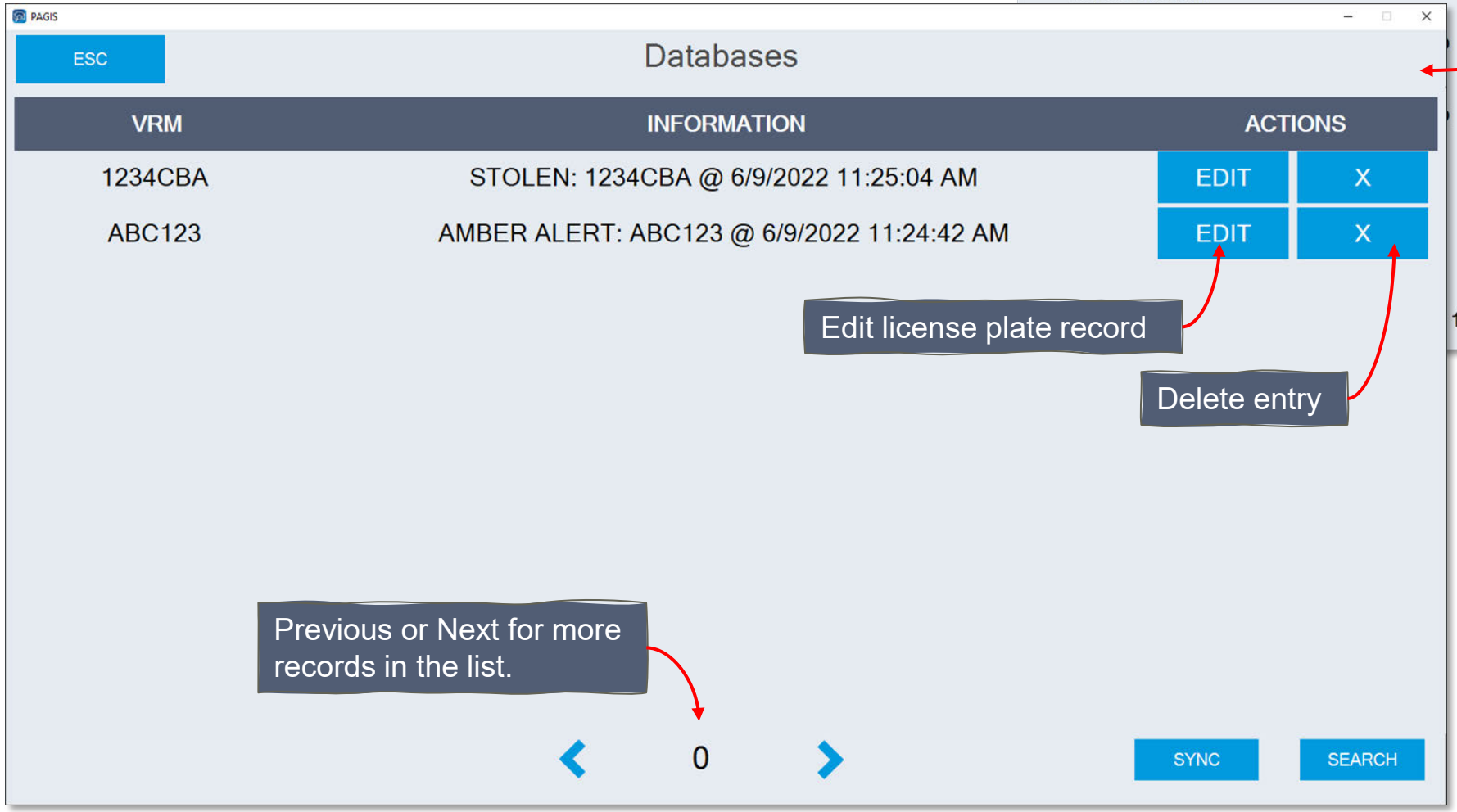
Sync- Begin/End Shift combined without data purge.

Search- Shortcut to Search Entry

Copyright © 2021 Neology, All Rights Reserved.

2871 Review- Edit Database 2 of 2





VIEW –Hotlist has two function based on origin of hotlist.

- Hotlist deployed to PAGIS via BOSS cannot be edited, only the hotplates list can be viewed. Editing/updates are indented to be managed via BOSS.
- Hotlist created in PAGIS, i.e., “Manual Reports” can be managed by PAGIS users, allowing for changes or deletion of the hotplates contained within the hotlist.

Copyright © 2021 Neology, All Rights Reserved.

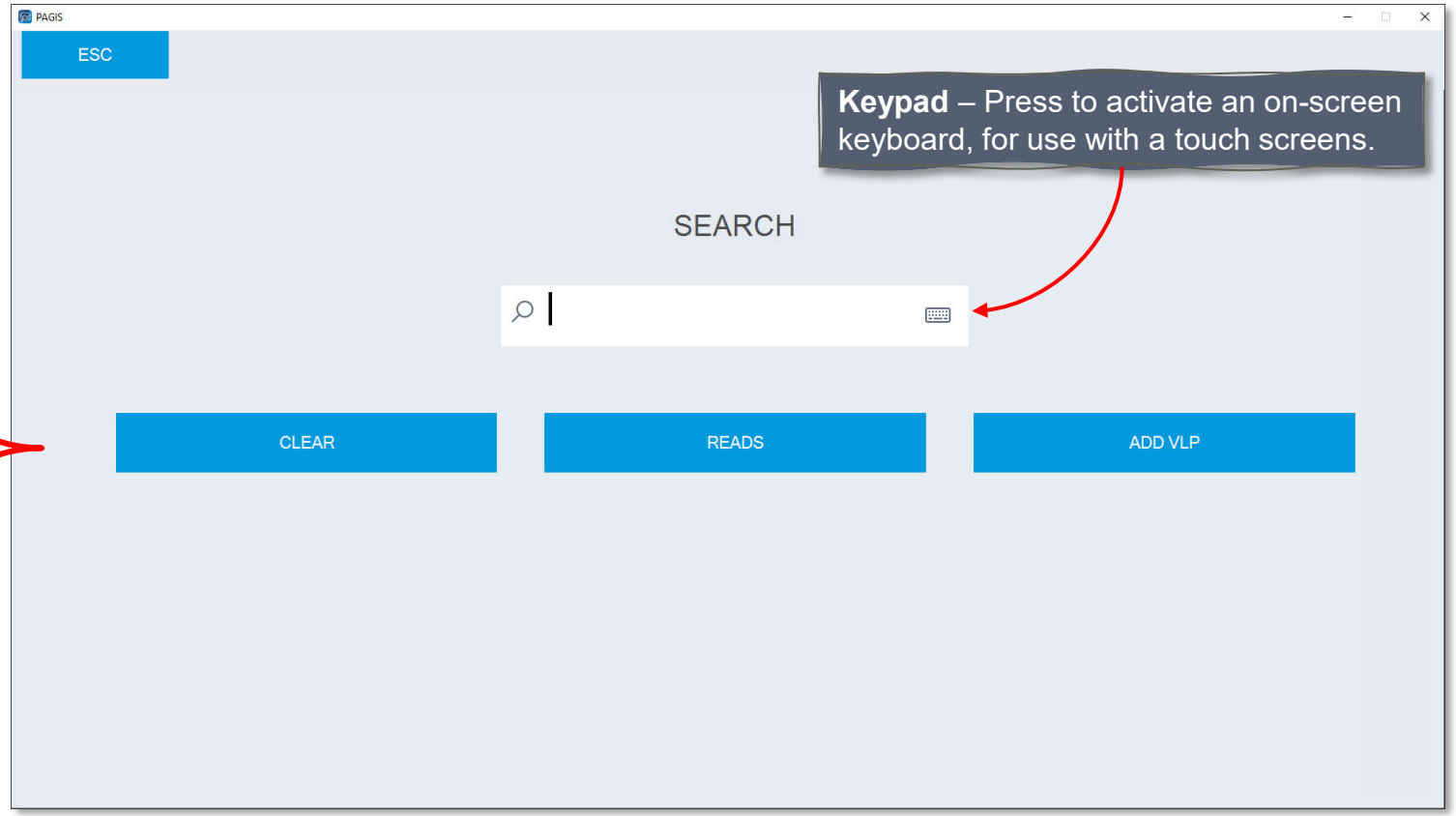
2872 Search Entry 1 of 3



Search Entry Button

Click Search Entry from the Main View screen to display Search features.

- **Text Field** – Enter alphanumeric string to search. Accepted wildcards are Asterisk “*” or Underscore “_”.
- **Clear** – Clear the content of the text box.
- **Reads** – Search for plate number with Reads and Hits currently stored in the PAGIS.
- **Add VLP** – Add hotplate to “Manual Reports” Alert List or check existing hotlist for the entered license plate. Partial plates or wildcards not accepted.
- **Esc** – Return to the previous screen.



Copyright © 2021 Neology, All Rights Reserved.

Search Entry- Reads 2 of 3

READS Searching against collected license plate data in PAGIS.

- Search criteria can include exact text or text and wildcards. Wildcards are special characters that represent any / all potential characters and can be used in searches and queries.

- Wildcard searches can be performed using the * and _ characters. The asterisk (*) designates an unknown number of characters while the underscore (_) indicates a single missing or unknown character. To search for a plate number with the characters 3 and C, entering *3_C* will display all records containing 3 and C separated by one character.



Copyright © 2021 Neology, All Rights Reserved.

Search Entry- Reads 3 of 3

2874

Save changes or Esc to return to Main View.
(Typ. thought out review screens)

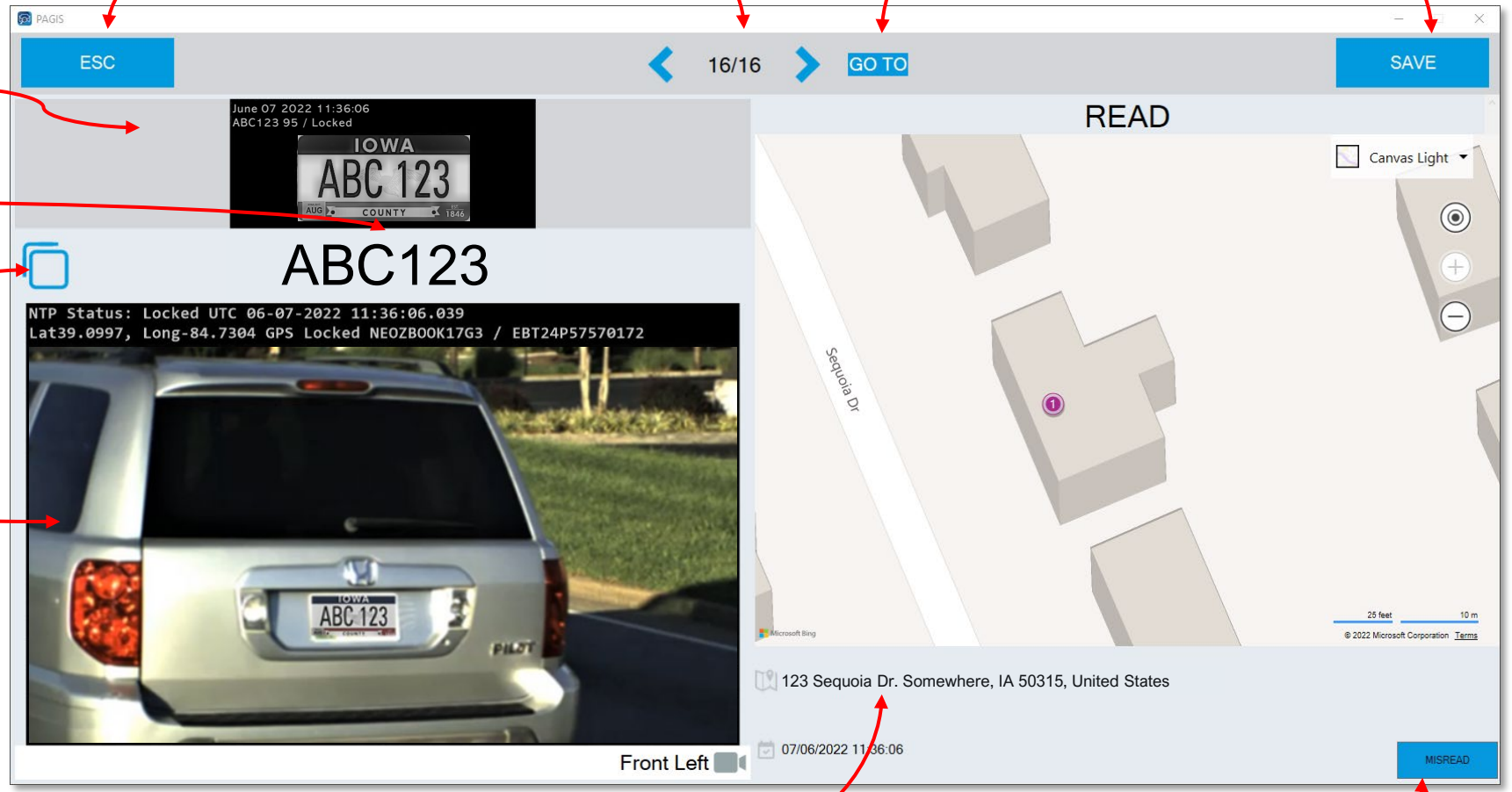
Current view / Total Reads.
Prev. & Next

Jump to specific read.

IR “Plate Patch” w/ NTP watermark
Clicking Plate Patch will result in larger view Of image.

OCR translation of “Plate Patch”
Click OCR Patch to correct a misread.

Copy plate number to clipboard



Color Camera “Overview” *w/ NTP status watermark.*
Clicking overview Patch will result in larger view of image.

Active Mapping with address translation.

Jump –Move to a specific record.

Copyright © 2021 Neology, All Rights Reserved.

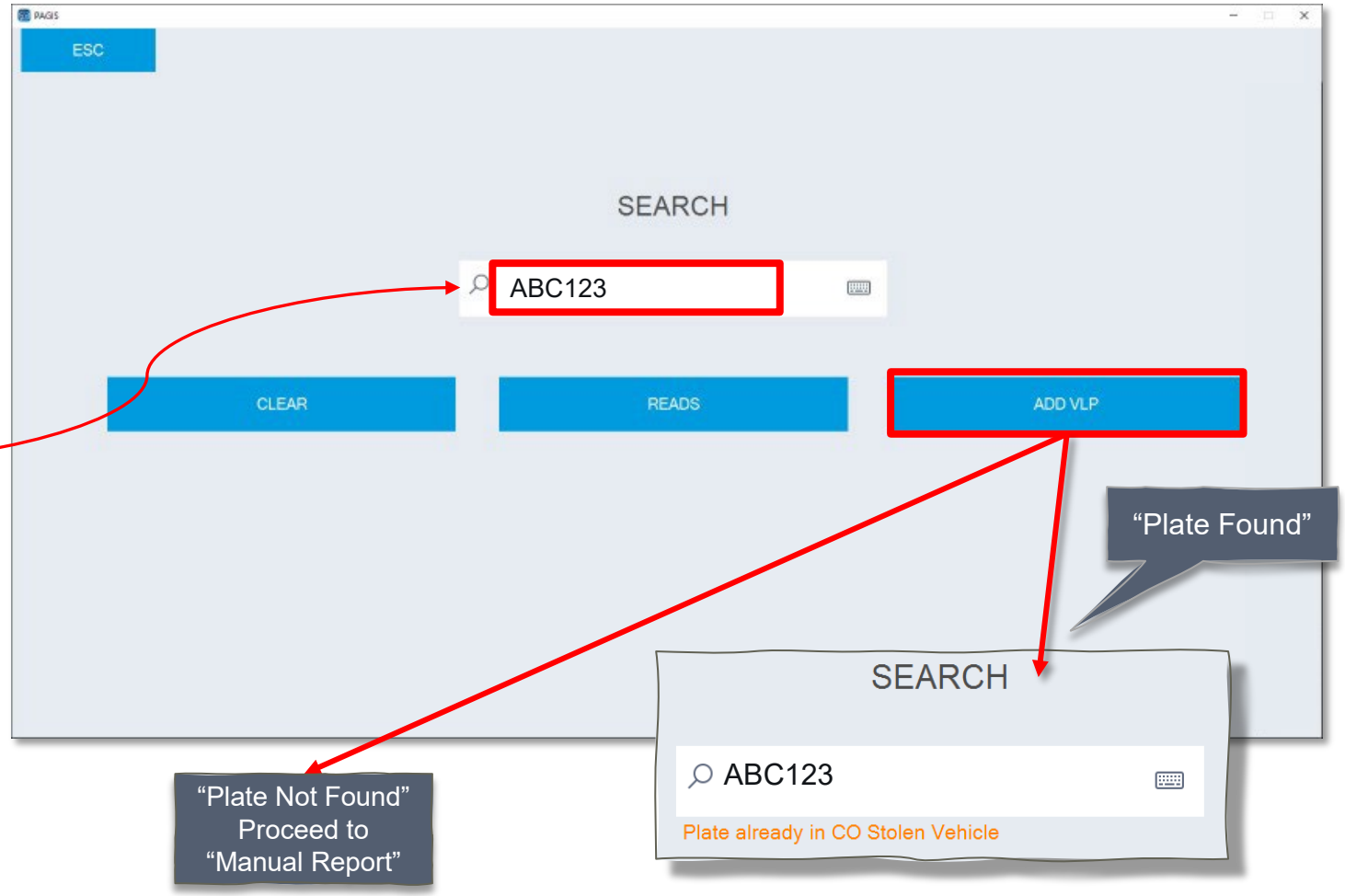
2875 Search Entry- ADD VLP 1 of 2

Add a plate to “Manual Reports” Hotlist or check for existence of plate in Hotlist download from BOSS.

- Manual Reports is a PAGIS standalone Alert List designed for manual entries by the PAGIS operator.
- Manual Reports Alert List do not transfer to BOSS or other mobile units utilizing PAGIS.
- Manual Reports Alert List are cleared out during a manual “upload” or during Purge cycle.

Enter plate into the text field, click “Add VLP”.

- If plate already exist, a message will applier indicating the Alert List it was found in. Otherwise, you will be prompted in the next screen to classify your entry.
- Wildcards or partial plates not accepted when adding hotplates.



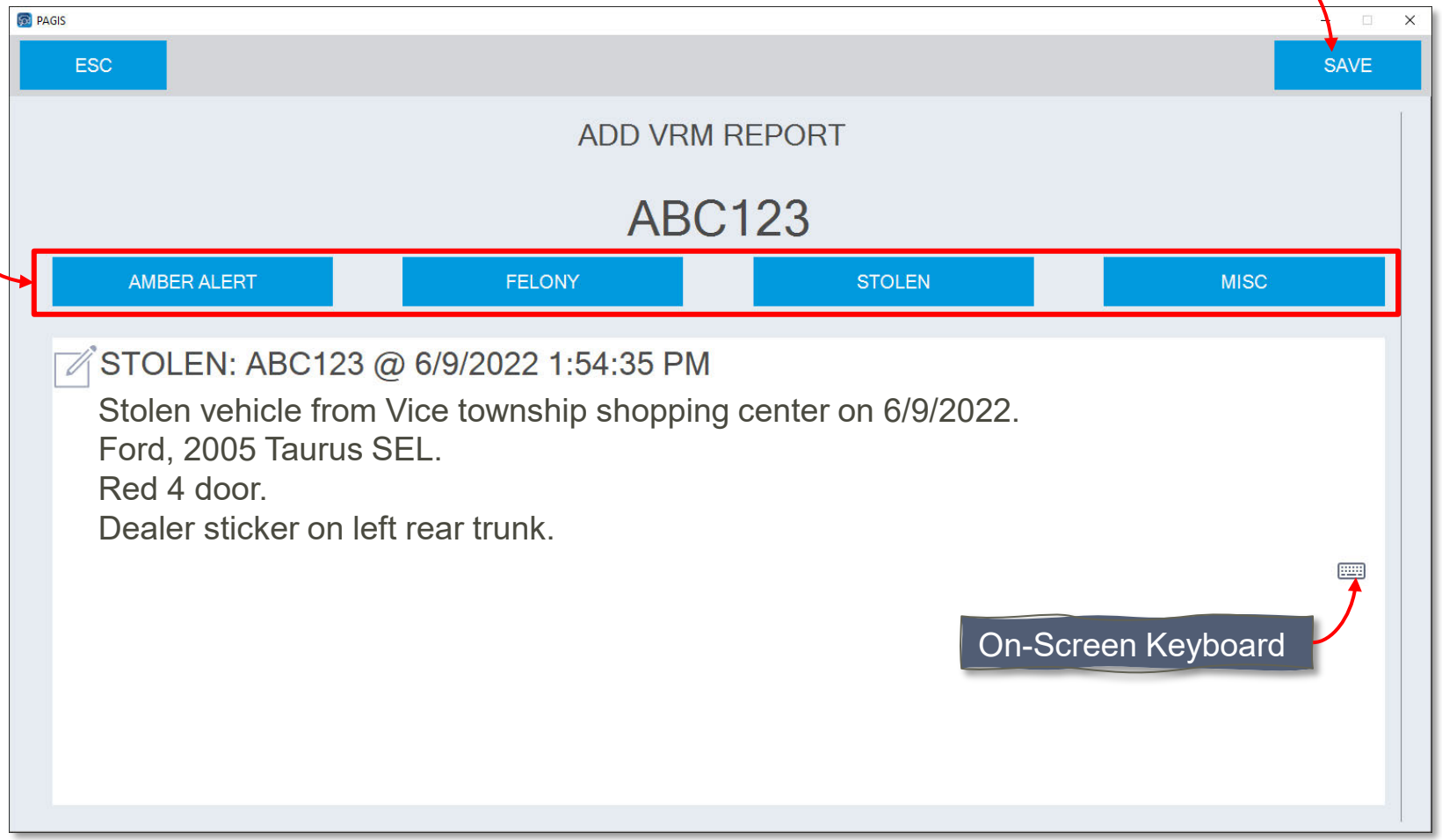
Copyright © 2021 Neology, All Rights Reserved.

Search Entry- ADD VLP 2 of 2

2876

ADD VLP Report:

- Select one of the four pre-defined classifications.
- Type in additional information about the vehicle.
- There is no limit to the number of manual entries that can be added to the Manual Report Alert List.
- Entries can be edited or deleted individually in the review Database section.
- All entries in the Manual Report Alert List will be discarded when a manual End Shift is performed.



Copyright © 2021 Neology, All Rights Reserved.

2877

End of PAGIS User Training



Thank you

Copyright © 2021 Neology, All Rights Reserved.

Recommended


NWS: Wintry mix possible in parts of CT tonight


Engagement: Wood-O'Sullivan


Trial of man accused of killing woman for her rings


Vote to seek CT funding for Torrington trail


Fairfield County's Giving Day fundraiser to end

NEWS // POLITICS

One CT town is adding license plate scanners at its borders. There are privacy concerns.


Julia Bergman

Updated: Dec. 19, 2022 8:42 p.m.



Subscribe Sign In

ONLY 99¢! Get Access to Your Trusted Source for Local News. ACT NOW



Federals funds have helped some municipalities expand the use of license plate readers.

Facebook/Bristol Connecticut Police Department

New Canaan recently became the latest Connecticut municipality to approve the use of license plate readers, with officials there citing an increase in stolen cars as the main impetus for purchasing the cameras.

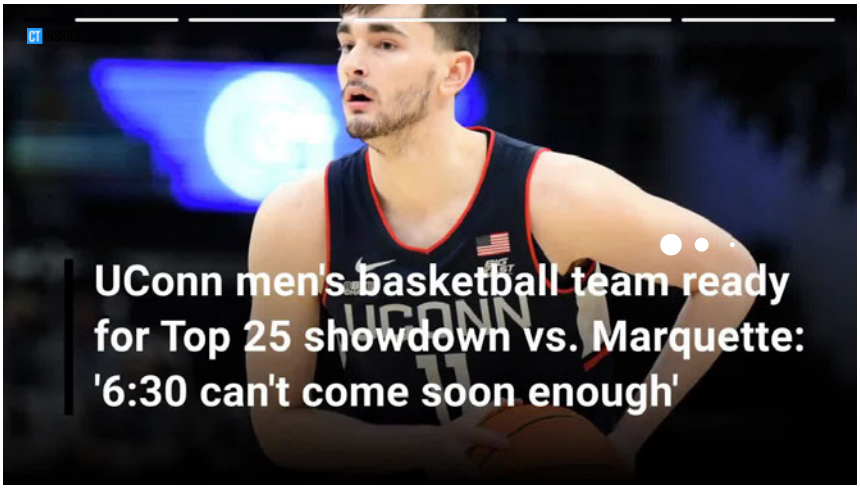
2879

ADVERTISEMENT
Article continues below this ad

This kind of surveillance technology has become prolific across Connecticut, with at least a handful of municipalities in the past year approving new license plate readers to be placed at stationary locations throughout towns or adding to their existing network of cameras.

In some cases, municipalities used federal stimulus funds to purchase the equipment, which enabled towns with smaller police budgets to acquire the technology and expedited the purchase of the camera systems in other cities.

ONLY 99¢! Get Access to Your Trusted Source for Local News. ACT NOW



New Haven is spending $12 million for 500 new video surveillance cameras and to expand its ShotSpotter gunshot detection system. New London and Norwich also purchased new camera systems. Stamford is installing 50 cameras at 30 different locations in the city. Glastonbury is also considering purchasing the devices.

"I'm definitely noticing more public displays of the use of surveillance technology in Connecticut. More and more towns are hopping on that bandwagon," said Claudine Constant, public policy and advocacy director for the Connecticut chapter of the American Civil Liberties Union.

Law enforcement and local officials who have approved funding for the systems have described the cameras as tools to help combat and solve crimes. Police have credited the cameras with helping to apprehend stolen vehicles, tracking down a missing person, and helping to arrest a juvenile suspect in a fatal shooting.

"Look at some of the challenges in law enforcement right now. There are staffing shortages pretty much across the board. These can be a bit of a force multiplier for us," said Town of Groton Police Chief Louis J. Fusaro Jr., a vice president of the Connecticut Police Chiefs Association. "They're like police officers at the corner that work 24/7, 365 days. They don't get sick. They don't get paid overtime."

But the networks of cameras in many towns and cities have generated privacy concerns from organizations such as the ACLU and residents. A 2019 report from the ACLU found that police in Fairfield, Westport, Stratford, Trumbull and Norwalk had helped U.S. Immigration and Customs Enforcement monitor "potential targets" through an extensive database of individuals and their locations collected by automated license plate readers.

ADVERTISEMENT
Article continues below this ad

2881

Fusaro said Flock Safety, one of the most popular private companies selling the readers, has a retention policy that automatically deletes the data after 30 days unless police indicate the information is part of an active investigation.

“We don’t want to surveil the public. The First Amendment is critical to us. We want to make sure we utilize technology in a way that’s ethical, legal and transparent,” he said.

The ACLU has also critiqued the opaqueness surrounding the technology’s use. For example, police in Connecticut are not required to detail how they are using the information nor where the cameras are located.

Some officials have announced generally where the cameras will be installed but not specified the exact locations. In Stamford, for example, the public safety director said the cameras would be “spread out throughout the city.” New Canaan officials said the readers will be placed at various, strategic locations around the town's borders. lack of transparency over how the technology is use.

ADVERTI EMENT
Arti le ontinues below this ad

At least 16 states have laws re ulatin the use of license plate readers or how the information collected from the devices is stored Some states prohibit the use of the devices except for limited public safety purposes or limit the types of investi ations

2882

in which they can be used. Others have mandatory privacy policies and limits on data retention.

MOST POPULAR

1. How a century-old law contributes to CT traffic
2. Former Plymouth principal faces termination, one administrator can return in child sex abuse case, official says
3. With rising electricity rates, some CT residents turning to third-party providers
4. What UConn women's basketball coach Geno Auriemma said about his technical foul: 'Dumb mistake by me'
5. David Borges: Our AP Top 25 men's basketball ballot for this week
6. Father of former CT resident Lindsay Clancy's children wrote eulogy for 'very difficult' funeral service
7. Great Wolf Lodge indoor water park breaks ground on new CT location

FIND THE BEST NEAR YOU

Guide to Legal Cannabis Dispensaries in CT

Going Solar in CT: Everything You Need to Know

How Much Does Solar Cost in CT?

How to Choose the Best Solar Company in CT

The readers capture the license plate number and every scan's date, time, and location. The information collected can be compared against a so-called "hot list," which can include the plate numbers of stolen cars and cars associated with Amber and Silver alerts.

The cameras have been a fixture on police cruisers in Connecticut for at least 10 years, but in recent years, more municipalities have installed them in physical locations such as on road signs, light poles and bridges.

Connecticut lawmakers have shown little interest in regulating the scanners. The Connecticut chapter of the ACLU advocated for legislation in 2012 and 2013 that would have required the deletion of license plate scan data, but the effort failed to get traction in the General Assembly.

It's unknown exactly how many of these readers exist throughout Connecticut as there's no reporting requirement for municipalities, so there's no centralized list detailing which cities and towns are using the technology. The cameras have also become popular with private businesses and homeowner associations.

Efforts at the local level to regulate the devices have also been unsuccessful. Constant, who previously served on the Hartford City Council, said several years ago, she was part of an effort to create a policy to regulate the hundreds of license plate readers throughout the city. But there "wasn't an appetite" among council members to impose any regulation or limitations on the use of the devices.

At the state level, Constant said the ACLU would continue to push lawmakers to allot more funding toward education, public health and economic growth, particularly as the General Assembly prepares to convene in early January for a budget-writing legislative session.

"A budget is a statement of values," Constant said. "To have lawmakers value people over surveillance and surveillance technology would be a beautiful thing."

Julia Bergman@hearstmediact com



Written By
Julia Bergman

Reach Julia on

Julia Bergman is a reporter with Hearst Connecticut Media Group. She covers Connecticut politics, including how public policy decisions affect the lives of residents here. She previously reported on the military for The Day newspaper in New London. A native of Philadelphia, Julia now calls Connecticut home, but won't give up her 215 area code

IN DEPTH COVERAGE

- **Former CT man charged in Tyre Nichols death focus of race debate**
- **Haar: CT's long-battling mortgage banker appeals to lawmakers**
- **As supermarket egg prices rise, demand soars at CT farms**
- **Owner mourns death of 60 animals killed in CT fire: 'Devastating'**

Camp Lejeune Check Compensation
Did you live or work at Camp Lejeune between 1953 1987? You may be entitled to compensation. Get a Free case review today
Camp Lejeune Justice | Sponsored
Click Here

2 Cards Charging 0% Interest Until 2024
With this card, you can focus on paying off your balance rather than your interest.
CompareCredit com | Sponsored
Learn More

1/2 Cup Of This (Before Bed) Can Melt Your Belly Fat Like Never Before
Healthy Guru | Sponsored

The Best Smartwatch for Seniors
★★★★★
Fitnus | Sponsored
Learn More

Born Before 1965? Here Are 19 Senior Rebates You Can Claim
TheWalletGuru.com | Sponsored

Getting 87¢ Generic Viagra Online Isn't Illegal, But CVS Doesn't Want You To
Public Health Forum by Friday Plans | Sponsored

Chuck Norris In His 80s Says Try This Once A Day For More Energy
Action Star Chuck Norris reveals his keys to getting more energy later on in life.
Roundhouse Provisions | Sponsored

Root Cause Of Female Hair Loss

2885
Hair La Vie | Sponsored

1 Simple Trick To Cut Your Electric Bill by 90% (Try Tonight)

★★★★★

Electric Saver com | Sponsored

Learn More

How To Remove A Hanging Belly

growthmax | Sponsored

If You Have Toenail Fungus Try This Tonight (It's Genius!)

WellnessGuide101.com | Sponsored

Watch Now

See the Savings Accounts our Nerds Love

NerdWallet | Sponsored

Learn More

A wearable ED device with no awkward interruptions

Eddie® is an ED device designed by medical professionals with medical-grade materials.

Eddie by Giddy | Sponsored

Man died in Colchester during tree-cutting accident, police say

ct insider

Stamford mom in court today after police say son found buried in Cummings Park

ct insider

Diagnosed with Non Hodgkin's Lymphoma or CLL?

Families affected may be entitled to compensation.

Select Justice | Sponsored

Learn More

If You're Battling Brain Fog, Low Energy or Anxiety?

Health Headlines | Sponsored

Learn More

Every Car Has It, But Most Have No Idea Where To Find It

Livestly | Sponsored

Government Will Now Install Solar For You If You Live In The e 12 States

Energy Bill Program | Sponsored

Learn More

Meet the Dexcom G6® CGM system

Dexcom | Sponsored

How a century old law contribute to CT traffic
ct insider

What UConn women's basketball coach Geno Auriemma said about his technical foul: 'Dumb mistake by me'
ct insider

The Fed is Meeting Soon, Lock in Your Rates Today
NerdWallet | Sponsored

Volvo Has Done It Again. This Year's Lineup Left Us Speechless. See It Now
Auto avings Center Search Ads | Sponsored
Learn More

These 2 Vegetables Will Kill Your Belly And Arm Fat Overnight!
Health & Wel are | Sponsored

HEARST newspapers
©2023 Hearst Media Services Connecticut, LLC

2888

MOTOROLA SOLUTIONS

Non-MSI LPR Camera Services (LinC), Fees and Payment Provision

I License Key:

The LinC Camera License Key (CLK) means an electronic license key that will permit the use of MSI's LPR software to be used with non-MSI branded / non-MSI issued LPR cameras (one CLK per camera) and select MSI Software Products.

II Offer Services:

This Offer includes the following Software Services / Software Products:

- LPR Software Services / Software Products:
- MSI Managed/Hosted LPR Account
- CarDetector Fixed LPR Software w/ all updates
- Target Alert Service
- Optional Services
- Cellular Data Service (Optional / Additional)

III Annual Service Fees:

The Service Fees applicable to each Annual Service Period for this Offer shall be as follows:

Annual Fee Schedule	
LinC CLK (Edge Camera)	$750.00
LinC CLK (Server Camera)	$500.00
Annual Cellular Data Plan per Camera (Optional)	$1,200.00

Customer/Agency Name	Massachusetts State Police
Name	Noah Pack
Title	Sergeant; ALPR Administrator
Email	noah.pack@pol.state.ma.us
Date	6/14/2023
Signature	Sgt. N. Pack #3680

Note: Form is acknowledged as representative of the standard fee schedule. No services, billing, fees, or costs are authorized or agreed to outside of formally quoted and approved purchases.

OPEN SOURCE FREE ONLINE RESOURCES

http://15q.net/

https://www.licenseplates.cc/

http://www.worldlicenseplates.com/

https://platerecognizer.com/

https://www.carfax.com/

https://www.carfaxforpolice.com/

https://www.kbb.com/vehicle-history-report/

https://www.mad4wheels.com/brands

http://mmr-demo.orpix-inc.com/detection/main/

https://www.autobytel.com/car-pictures/

https://ring.com/neighbors

https://www.bing.com/images/trending?form=Z9LH

https://www.vehiclehistory.com/

https://carnet.ai/

https://osintcurio.us/2021/02/17/cosint-osint-on-cars/

https://infotracer.com/plate-lookup/



neology™
mobility [re]imagined™

PAGIS Administrator's Manual

Version 2.14

Updated 7/16/2020

2892

Table of Contents

Table of Contents ____ *2*

NOTICES ____ *4*

Technical Support ____ 4

Design Changes ____ 4

Trademarks ____ 4

Copyright ____ 4

Version ____ 4

INTRODUCTION ____ *5*

1.1 Dual Lens Color and Infrared Camera ____ 5

1.1.1 Available Products ____ 5

1.2 Using This Manual ____ 6

SCREEN REFERENCE ____ *7*

2.1 The PAGIS Software Login Screen ____ 7

2.1.1 Logging on with the Default Administrative Account 7

2.2 Main Screen - Live View ____ 8

2.2.1 Getting Started in PAGIS ____ 8

2.3 The PAGIS Navigation Buttons ____ 9

2.3.1 Camera Control Buttons ____ 9

2.3.2 GPS Indicators ____ 10

2.3.3 Camera Firmware Update (Restricted Users) ____ 10

2.3.4 Day/Night Mode ____ 10

2.4 Begin Shift ____ 11

2.4.1 Sync via USB Thumb drive (or Local Source) ____ 11

2.4.2 Sync via Wireless Network ____ 11

2.4.3 PAGIS Auto-Sync Settings ____ 11

2.4.4 Begin Shift – Additional Information ____ 11

2.5 End Shift ____ 11

2.5.1 Sync to BOSS ____ 11

2.6 Cam Mode Button ____ 12

2.6.1 Camera Modes ____ 12

2.7 Taking a Picture ____ 12

2.8 Search Entry Screen ____ 13

2.8.1 Searching Synchronized Hotlists for License Plates 13

2.8.2 Searching Locally Stored Reads and Hits ____ 13

2.8.2.1 Searching for a Match ____ 14

2.8.3 Wild Card Symbols ____ 14

2.8.4 Manually Adding a Plate to PAGIS ____ 15

2.8.4.1 ADD VLP Query ____ 15

2.8.4.2 ADD VRM Report Screen ____ 15

2.9 The Review Screen ____ 16

2.9.1 Summary Review Section ____ 16

2.9.2 Review Navigation Buttons ____ 16

2.9.3 Reads ____ 17

2.9.3.1 Reads Result Screen Navigation Buttons ____ 17

2.9.3.2 Interactive Buttons – Reads Screen ____ 17

2.9.4 Hits ____ 18

2.9.4.1 Hit Screen Attributes ____ 18

2.9.4.2 Hit Screen Function Buttons ____ 19

2.9.4.3 Interactive Buttons – Hits Screen ____ 19

2.9.4.4 Set Disposition – Additional Detail ____ 19

2.9.4.5 Add Intel – Additional Detail ____ 20

2.9.5 Misreads ____ 20

2.9.5.1 Marking a Record as a Misread: ____ 21

2.9.6 Audits ____ 22

2.9.7 Targets ____ 22

2.9.7.1 The Targets Screen ____ 23

2.9.7.2 Targets Screen Navigation Buttons ____ 23

2.9.8 Databases ____ 24

2.9.8.1 Databases Screen Functions ____ 24

2.9.8.2 Databases Screen Navigation Buttons ____ 24

2.9.8.3 Databases Edit- “Manual Reports” ____ 25

ADMIN SETTINGS ____ *26*

3.1 Sync Options Screen ____ 26

3.1.1 Synchronization Types ____ 26

3.1.1.1 Synchronization to Disk (Local Storage) ____ 27

3.1.1.2 Synchronization with BOSS ____ 27

3.1.1.3 Sync to “Instation” (Formerly BOF2 and BOF3) ____ 28

3.1.2 Global Sync Options ____ 29

3.2 PAGIS Privacy Settings (Local Data Retention) ____ 30

3.3 Language ____ 31

3.4 Location ____ 31

3.5 Users ____ 32

3.5.1 User Privileges ____ 32
3.6 Sound ____ 33
3.6.1 Configuration Buttons ____ 33
3.7 System ____ 34
3.8 Rules ____ 35
3.8.1 Rules – Additional Clarifications ____ 35
3.9 OCR ____ 36
3.10 External ____ 37
3.10.1 XML Datastream Ports ____ 37
3.11 Cameras ____ 38
3.11.1 Checking the Connection ____ 38
3.11.2 Troubleshooting Camera Connections ____ 38
3.11.3 Configuring the Cameras in PAGIS ____ 39
3.12 Cam Setup ____ 40
3.12.1 Cam Setup Navigation Buttons ____ 40
3.13 Configs (Camera View Modes) ____ 41
3.13.1 Configs Navigation Buttons ____ 41
3.13.2 Reviewing and Modifying Existing Modes ____ 42
3.13.3 Adding a New Camera Mode ____ 43
3.14 Info ____ 44
3.15 Camera Firmware Update, (Admin) ____ 44
PAGIS INSTALLATION GUIDE ____ 45
4.1 PAGIS System Requirements ____ 45
4.2 PAGIS Prerequisites ____ 45
4.2.2 PAGIS Software Installation (MDC) ____ 46
4.2.3 PAGIS Software Installation (Mobile Processor) ____ 47
TROUBLESHOOTING TIPS ____ 48
5.1 Troubleshooting & Tips ____ 48
5.1.1 PAGIS with NetMotion VPN ____ 48
5.1.2 Cisco VPN Client: ____ 48
5.1.3 Microsoft .NET 3.5 Installation ____ 48
5.1.4 Firewall Settings for Client-Server Installations ____ 48
PAGIS/BOSS3 CONFIGURATION ____ 49
6.1 Creating a New Device in BOSS3 ____ 49
6.2 Enabling a New Mobile System in BOSS3 ____ 49
6.3 Assigning Ownership to a Device in BOSS3 ____ 49
6.4 Assigning Hotlists to a Device in BOSS3 ____ 50
PAGIS/BOSS4 CONFIGURATION ____ 50
7.1 Creating a New Device in BOSS4 ____ 50
7.2 Enabling a New Mobile System in BOSS4 ____ 50
7.3 Assigning Ownership to a Device in BOSS4 ____ 51
7.4 Assigning Hotlists to a Device in BOSS4 ____ 51
APPENDIX A: THE GLOSSARY ____ 52
APPENDIX B: PAGIS SOFTWARE DATABASE FILE ____ 53
APPENDIX C: FAQ ____ 55
APPENDIX D: XML DATASTREAM ____ 60

2894

NOTICES

The information within this manual is authorized for distribution to customers, authorized service center personnel, and distributors of Neology. Every effort has been made to supply correct information. However, Neology assumes neither responsibility for its use, nor for any infringements of patents or other rights of third parties, which may result from its use. No license is granted by the manufacturer under any patent or patent rights. Neology reserves the right to modify and update the equipment at any time without prior notice. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means to a third party without the prior consent of the copyright holder. The manufacturer's warranty will be invalidated if untrained personnel operate the equipment or if any attempt is made to service the equipment by unauthorized personnel.

This manual contains confidential and proprietary information and should not be redistributed except as needed for proper use and maintenance of the agency's Mobile ALPR system.

Technical Support

Service of this equipment by replacement of parts, on-site repair, routine maintenance inspection, and scheduled remote support session is available. Please contact Neology ALPR Technical Support.
Phone: (833-747-7577), Option 2
Support Team Email: Alpr_support@neology.net
For Customers in Europe, Middle East and Africa: Support@PIPSTechnology.co.uk
Web: www.neology.com
Fax: 858-391-0264
Corporate Office: 13520 Evening Creek Drive Suite 460. San Diego, CA 92128

Design Changes

Neology reserves the right to change the design of any product from time to time without notice and with no obligation to make corresponding changes in products previously manufactured.

Trademarks

Neology™ is a trademark of Neology Inc., and either registered or pending registrations in several jurisdictions. Windows, Windows 7, Windows 8, Window 10, and .NET are all trademarks of the Microsoft Corporation. Other trademarks and registered trademarks are the property of their respective owners.

Copyright

The Neology PAGIS Software is copyright of Neology. All rights reserved. This product contains confidential and trade secret information of Neology and is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portions of it, may result in civil and criminal penalties.

Version

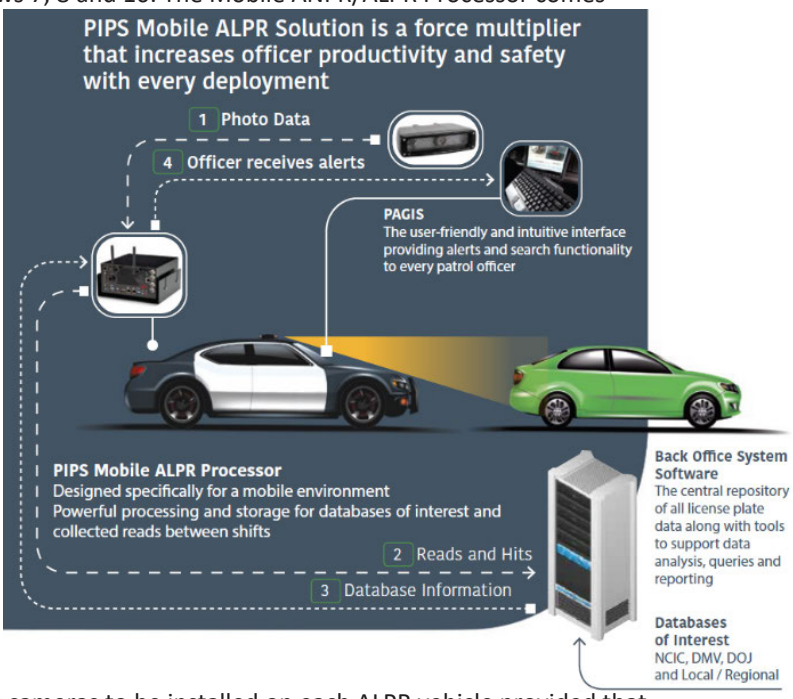
This manual demonstrates the attributes of the Neology PAGIS Software Version 2.14 and was last updated in April 2021.

2895

INTRODUCTION

Neology's Automated License Plate Recognition (ALPR) software solution called PAGIS utilizes dual-channel, dual-lens, cameras to "read" plates. Our software is optimized to run on the Mobile Processor itself or in conjunction with a mobile data computer (MDC). Our mobile software is compatible with Microsoft Windows 7, 8 and 10. The Mobile ANPR/ALPR Processor comes equipped with Microsoft Windows 10 Embedded.

The PAGIS Software processes the infrared plate image provided by any of the cameras and then interprets the plate number through Optical Character Recognition (OCR) via the mobile processor. The PAGIS application then searches for any matches of the plate with those listed in the databases, or "hotlists," distributed from the Back Office System Software (BOSS) or other external sources.



WARNING: To reduce the risks associated with impact, which if not avoided, could result in serious injury or death: Do Not interact with the ALPR system while driving in hazardous situations. The PIPS mobile camera series and License Plate Capture Software are not intended for use in hazardous environments, so that the User and/or others are not put at risk for personal injury and/or property damage.

1.1 Dual Lens Color and Infrared Camera

The Mobile ALPR System allows for a maximum of four (4) dual-lens cameras to be installed on each ALPR vehicle provided that the vehicle supports the additional mounting equipment.

Each dual-lens mobile camera uses visible light to take color overview pictures of the vehicle and uses infrared (IR) illumination to capture the license plate's alphanumeric characters. IR illumination offers the best capture performance of reflective license plate characters for the following reasons:

- State issued license plates are designed to be highly reflective to IR light.
- Cameras using IR capture technology do not depend on the presence of visible light to function.
- Cameras using IR capture technology are not negatively impacted by the effects of headlights, solar glare, or total darkness.
- IR light penetrates rain and fog better than visible light.
- Due to these attributes, the system can be used 24 hours a day, seven days a week.

1.1.1 Available Products

Additional information about this and other Neology applications, cameras, and solutions are available on the PIPS web site: http://www.pipstechnology.com

1.2 Using This Manual

The section overview of this software manual is as follows:

Section 1: The Introduction and Basics

Section 2: PAGIS User's Section: Explains screen function and User Operations in the PAGIS Software

Section 3: Troubleshooting Tips

Section 4: Software Administrator's Guide: Explains how to install and configure the PAGIS Software

Section 5: Additional Information and Troubleshooting Tips

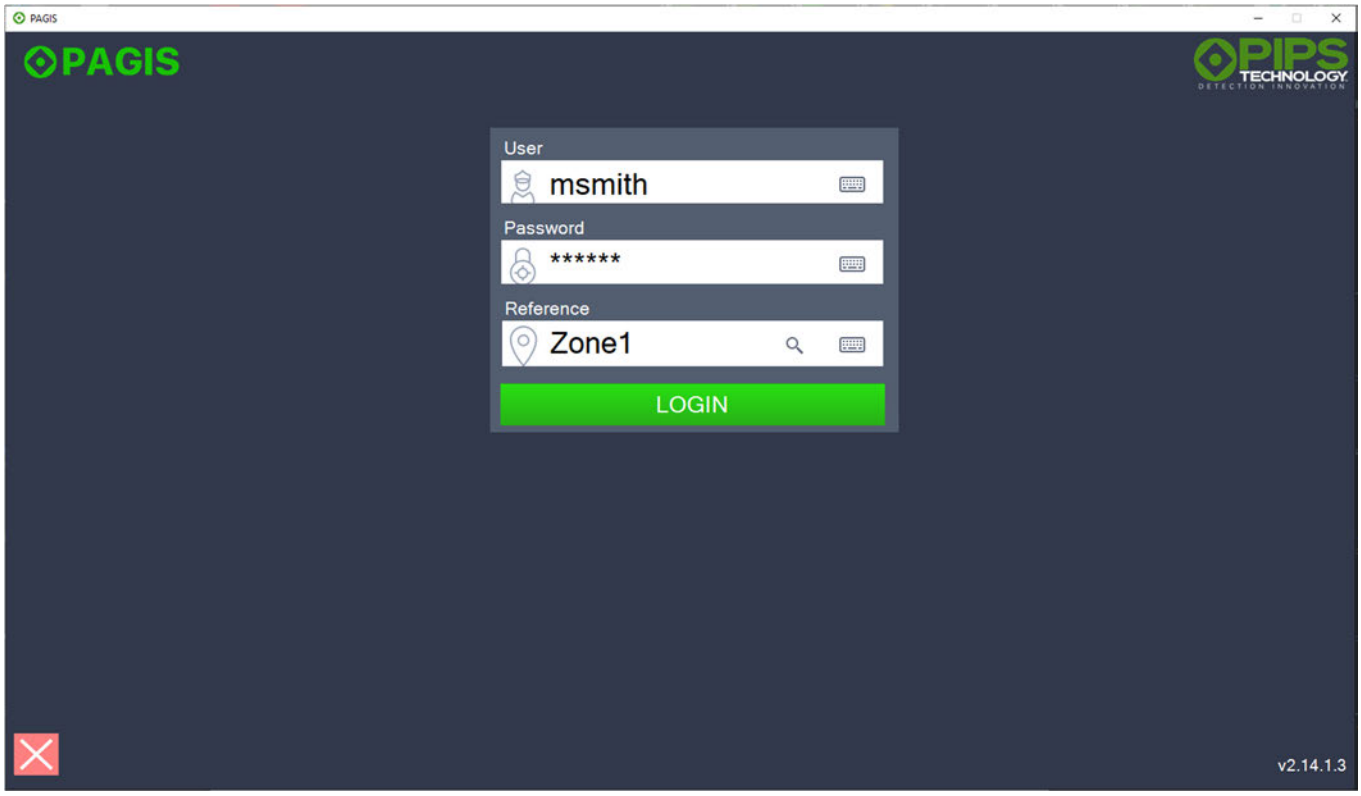
Section 6: Initial BOSS configuration for new PAGIS devices (MDCs)

Appendices: Additional features and details

2897

SCREEN REFERENCE

This section guides the user through the PAGIS Software screens and the available options. Screens are grouped according to function. When a button is grayed out or missing, the option is not available, or no information has been accrued to activate it.



2.1 The PAGIS Software Login Screen

The PAGIS Software allows users with various access privileges to use the same MDC. For users with touch screen monitors, the Keypad button immediately to the right of any text box gives the user access to an on-screen keyboard for data entry.

User Field: The alphanumeric string assigned to identify the user. Usernames are not case sensitive.
Password Field: Password of the assigned user logging in. Passwords are case sensitive.
Reference Field: This is an optional field utilized to fit a number of use cases. A user can manually enter a reference at logon, leave the field blank, or select list of unique tags that will be associated with all data captured while logged in. If the Administrator has configured a default reference tags, that information will be displayed automatically. Otherwise, it will be blank.
Login Button: Submits the username and password to attempt a login.
Exit Button: By clicking the X icon in the lower left-hand corner, the user can exit/close the PAGIS Software.

2.1.1 Logging on with the Default Administrative Account

The PAGIS Software includes a default administrative account that can be used for the initial configuration. To do so, simply click the **Login** button with the User and Password fields blank.

NOTE: System Administrators are strongly encouraged to configure users for PAGIS just before, or soon after the installation and setup. PAGIS users accounts are created and maintained in BOSS. Once Users are established by the BOSS System Administrator, the default user account is automatically disabled. Best practices are to be certain at least one User account has administrative privileges.

2.2 Main Screen - Live View

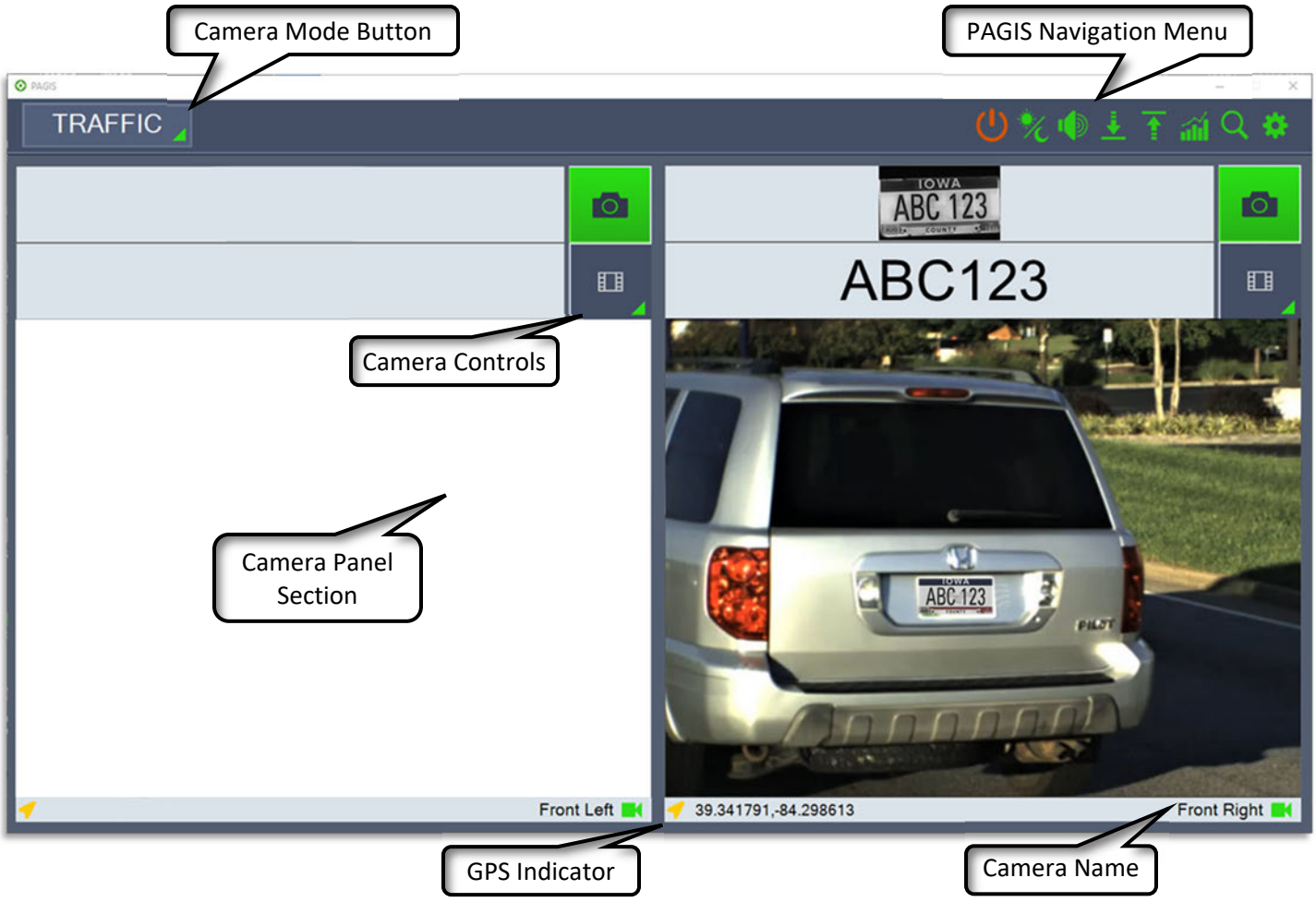
Upon a successful login, the user will see the Main screen (Live View). This is the default view and starting place of all PAGIS Software features. (NOTE: Access to features is based on user group rights established in BOSS.)

The Main Screen is also the place users will monitor read images and ALPR “hits”. At the initial startup of the system it is normal to see only a blank/grey screen for a few seconds. Once a connection has been established with the mobile cameras, white boxes will be displayed showing the live-feed camera panels. At this point, the system is ready to capture reads/plates.

2.2.1 Getting Started in PAGIS

By default, PAGIS loads into a static view. This means live video will not automatically appear in the camera panels (white boxes) until a plate has be captured or the user selects one of the live feed options.

Once a plate is “seen” by a camera assigned to the current viewing mode (Traffic vs Parking), it will display the captured information in the corresponding camera panel. Each plate capture is also accompanied by a short “Beep” to audibly alert the user a read has taken place. (NOTE: If the user is in the Traffic Mode at the time a parking camera reads a plate, there will be a sound effect, but no plate image will be displayed on screen unless that plate is on a synchronized Hotlist or until the user switches to Parking Mode.)



2.3 The PAGIS Navigation Buttons

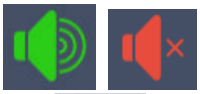
This section provides a quick reference guide to the available navigation buttons of the Live View screen.



The Camera Mode button is located in the upper left corner and is used to switch between the configured camera modes. Once configured, the name will change to a selected mode. The default values are “ALL”, “Traffic” and “Parking”.



The Logoff button is located in the upper right of the window. When selected, the user will be logged out of PAGIS and return to the login screen.



The Sound button is located to the right of the Logoff button. When selected, this button with toggle the PAGIS system sounds On and Off.



Day/Nite mode switches PAGIS between day & night mode screen skins.



The Begin Shift Synchronization button is located to the right of the Sound button. When selected, this will reach out to the BOSS server to download users, hotlists, and other system settings.



The End Shift Synchronization button is located to the right of the Begin Shift Button. When selected, this will upload any previously unsent reads, images, and audits to the BOSS server.



The Statistics/Review button is located to the right of the End Shift Button. When selected the user is able to review Databases/Hotlists, Reads, Targets, and other PAGIS information.



The Search button is located to the right of the Review Button. When selected the user can search his/her reads as well as manually add a license plate to a temporary hotlist.



The Admin/Settings button is located in the upper right corner of the screen. This button is only viewable to Admin level users and allows for system configuration changes and setup.



Firmware update icon will atomically appear when PAGIS detects a new firmware is available for the P720 mobile cameras. All user types are notified, but only Admins can apply the update.

2.3.1 Camera Control Buttons

The dual-lens cameras can capture both color and an infrared image. Formerly, there were a total of three buttons that allowed the user to view the IR and color feed as well as capture a picture directly from PAGIS. Now there is a toggle button to switch between color and IR views and a separate button to take a picture. These buttons are displayed on the main Live Screen as shown below:



The Camera View Selector button: This is the default state at login showing the Static View. (**NOTE**: PAGIS does not automatically display a life feed.)



Color View: by clicking on the Camera View Selector button once, the user will switch to the Color View Mode. This displays the current view of the color camera and will time out after 60 seconds.



IR View: by clicking on the Camera View Selector button twice, the user will switch to the Infrared (IR) View Mode. This displays the current view of the IR camera and will time out after 60 seconds.



The Take Pic button: Just above the Camera View Selector button is the “Take Pic” button. This button allows the user to quickly take a picture from the camera currently viewed.

2.3.2 GPS Indicators

GPS is stamped on each read and hit as capture events take place by the system. The signal strength and location indicators are located underneath the camera panels at the bottom of the Live Screen.

39.341788,-84.298518 Shows an example of the Location Indicator displaying the Lat/Long on the most recent read

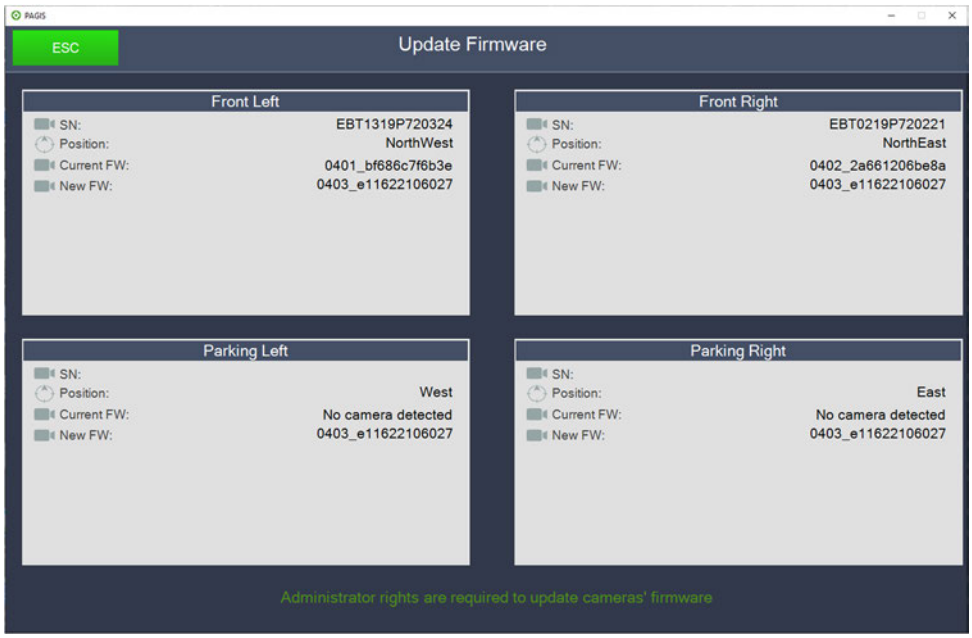
A green or yellow indicator shows a strong or medium strength GPS lock.

A red indicator shows there is no available GPS information.

2.3.3 Camera Firmware Update (Restricted Users)

Camera firmware update provides a means for Neology to update the camera software to enhance and or correct camera performance. The frimware icon will only apper when update is avialable.

- The firmware update process only updates camera that are attached and function on the mobile processor.
- Restricted PAGIS users are only notified and displayed update information, only a PAGIS administrator can apply the FW update.

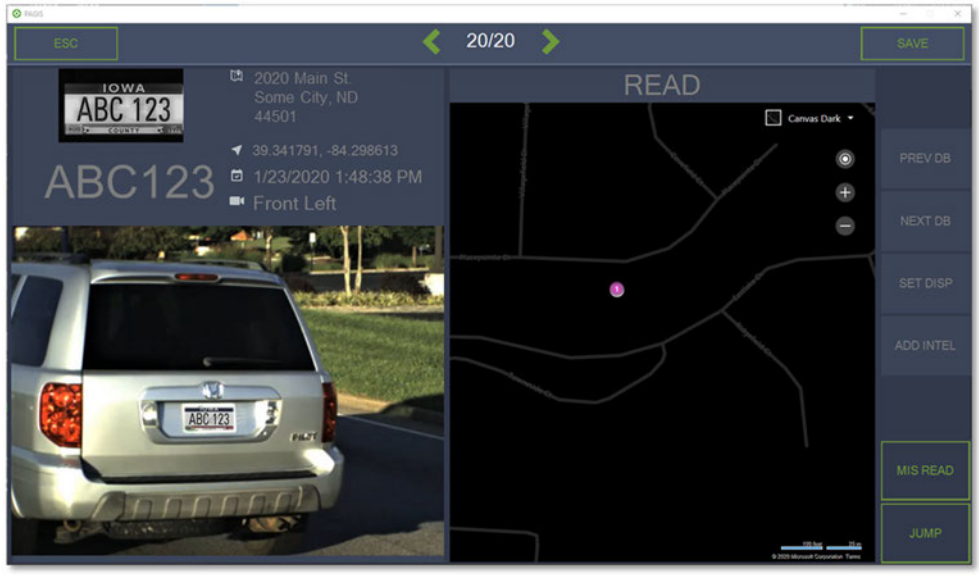


Firmware Updater Window List.

- Title “Camera Name”.
- Camera serial number.
- Position.
- Current FW version.
- New FW version available.

2.3.4 Day/Night Mode

Day/Night mode changes PAGIS user interface skins to a darker appearance to reduce illuminating the vehicle interior.



2901

2.4 Begin Shift

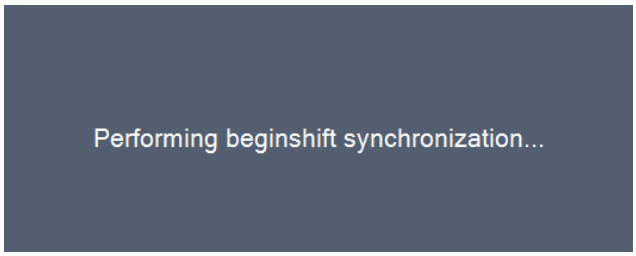
Begin Shift is thought of as the first step for all PAGIS users. From the Live View Screen, the PAGIS user must click the Begin Shift button twice. Once to select the function and once more to launch the Sync. With most agencies, this action utilizes a wireless network to import all the necessary data used during a shift (Hotlists, Dispositions, and Targets) directly from the BOSS Server. However, agencies can also configure their systems to perform this function via Thumb drive or a local source file.

2.4.1 Sync via USB Thumb drive (or Local Source)

Depending on the agency network, some alter the default PAGIS/BOSS configuration mode to use a USB Thumb drive or locally stored file on the MDC/Laptop instead of the wireless Sync. In order to synchronize effectively, the user must first confirm he/she has access to the source location before initiating Begin Shift. **NOTE**: All synchronizations using this method must be performed manually. To learn more about this process, refer to the "Client Tools" section of the BOSS Manual.

2.4.2 Sync via Wireless Network

Synchronizations over a wireless network provide the agency with additional automated features. Best practices recommend the user manually launch Begin Shift from the Live View Screen at the beginning of every patrol shift. However, it is possible for users to allow PAGIS to synchronize via its auto-sync settings. When a manual Begin Shift is launched, the Main View Screen removes the camera feeds and displays a status window of the Sync process. Once the Begin Shift operation is complete, PAGIS will return to the normal Main View Screen.





2.4.3 PAGIS Auto-Sync Settings

PAGIS auto-sync settings are best thought of as how PAGIS receives additional updates and maintains the downloaded ALPR data throughout the entire patrol shift. This prevents the need for the officer to manually perform Begin Shift functions multiple times a day. The auto-sync occurs every 30 seconds and receives data in small batches. The batches are not to exceed 1MB in size for every minute of download. In addition to receiving data, the auto-sync function also uploads a copy of data collected by PAGIS and sends it to BOSS for reporting/processing.

2.4.4 Begin Shift – Additional Information

By default, the synchronizations in PAGIS receive only what has been changed to the ALPR data since the last Sync. Meaning, if some plates have been removed from a Hotlist and others have been added, the system will only transfer that data instead of downloading the entire Hotlist each time the Begin Shift is launched. This helps to reduce the amount of data transferred over the agency's network. **NOTE**: Begin and End Shift synchronization, as well as all auto-sync features, are dependent upon stable communication to the BOSS server via an active data connection.

2.5 End Shift

End Shift in PAGIS is the process in which all the collected ALPR data (Reads, Hits, and Images) from the recent shift is uploaded to the BOSS server and cleared from the local cache. As with Begin Shift, the agency has two options. They can choose to Sync via USB Thumb drive or via wireless connection. Best practices recommend users perform an End Shift Sync at the end of every patrol.

2.5.1 Sync to BOSS

At the end of every shift, the accrued ALPR data should be exported to BOSS. Just like with Begin Shift, the user must click the button twice to launch it (once to select it and once more to execute the Sync). During the Sync, PAGIS uploads any Reads, Hits, and Images not already synchronized to BOSS and purges these items from the local cache on the MDC's hard drive. Completing an End Shift also removes any VLP entries manually added to PAGIS during the shift.

2902

2.6 Cam Mode Button

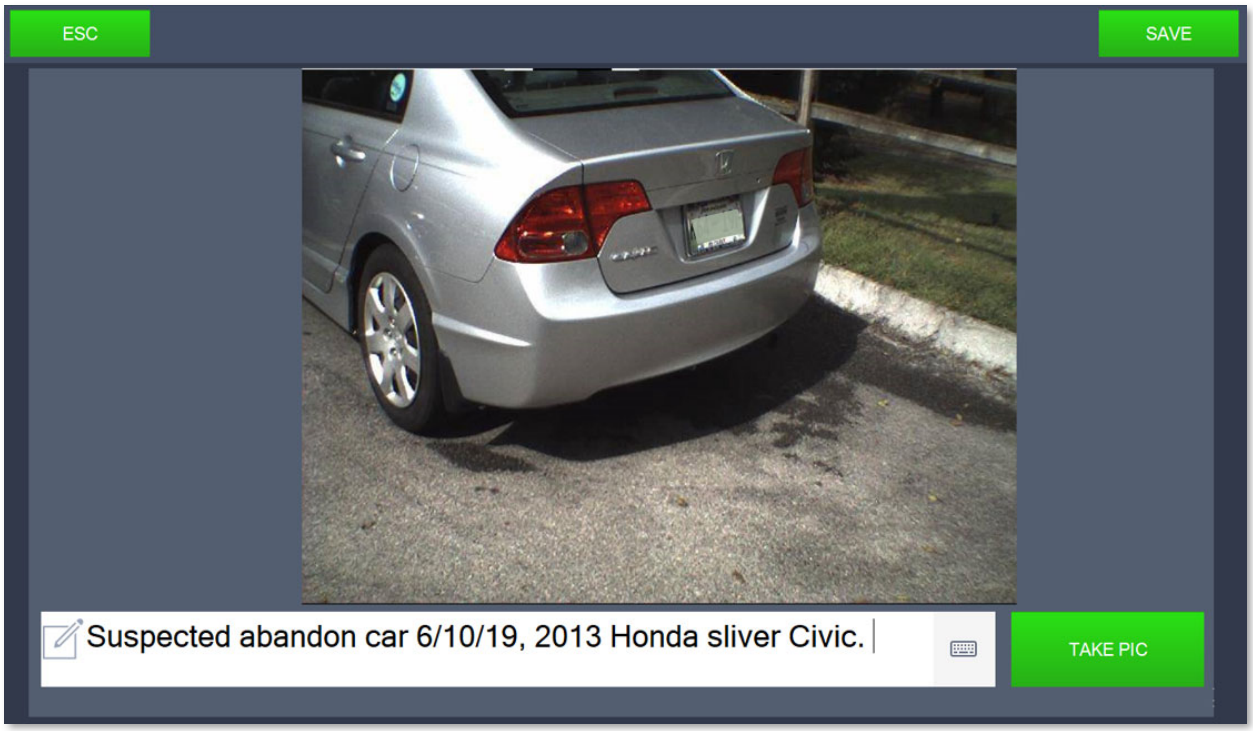
Clicking the Cam Mode button in the upper left corner of the Live View Screen allows the user to cycle through the different camera modes configured by the PAGIS Administrator. Changing the camera mode changes which cameras are displayed on the Main Screen.

2.6.1 Camera Modes

By default, PAGIS provides “Parking” and “Traffic” as the two configuration modes. Users often switch these modes to suit their current use-case. For example, an officer in a parking lot will often switch the mode to “Parking” so s/he can see the parking cameras on the Live View Screen. They can then switch back to “Traffic” when monitoring city streets.

2.7 Taking a Picture

The PAGIS software has ability to quickly take a picture from one of the currently displayed ALPR cameras on the Live Screen. The user only needs to click on the Take Pic button. 



To Take a Picture:

1. From the Live View Screen, press the Take Pic button from the desired camera
2. The image taken will be displayed
3. Enter a description of the picture in the text field at the bottom of the screen
4. Press Save to save the picture or Escape to cancel. Either action will return you to Live View.

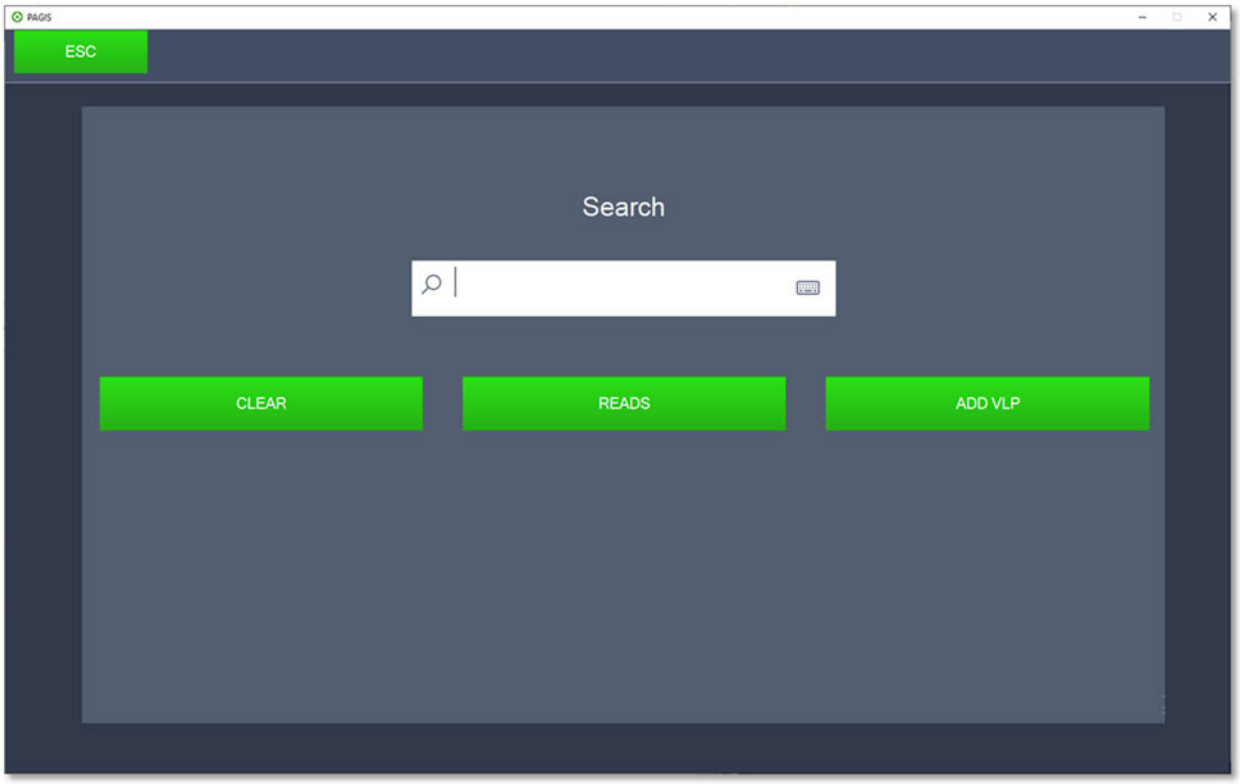
NOTE: The picture will Not be saved if a description/note is not entered in the text box.

To View the Saved Images:

1. Navigate to the Review menu in PAGIS
2. Select Audits
3. The user will be able to see a thumbnail of the image and the saved text/note
4. In order to review the saved images at a later time, the user will need to run the Audit Report from BOSS.

2.8 Search Entry Screen

Pressing the Search button icon from the Live View screen or SEARCH from the Databases window allows the user to search all manually entered plates as well as all BOSS synchronized databases (Hotlists) for license plate and target information. Users can also search all locally stored reads/images accrued since the last End Shift by clicking the Reads button instead of pressing the Enter key.



2.8.1 Searching Synchronized Hotlists for License Plates

By entering a vehicle license plate number (VLP) and pressing the Enter key or the ADD VLP button, the user can quickly search all the stored plate information locally collected as well as the information from all synchronized hotlists distributed from the BOSS server. **NOTE**: Hotlists can only be searched by entering complete VLPs. Wildcards and partial plate numbers will not return results.

Search Box: The text field used to enter the desired plate search via alphanumeric characters and/or wild card symbols.

Clear Button: Clears the contents of the search box.

Driver's License Info: The search field can also check the Hotlists for any DL information stored (Not available all countries).

Reads Button: This button searches for a match from all the reads/hits locally stored on the MDC/Laptop.

ADD VLP: Searches all locally stored hotlists for the plate and if there's no match, allows the user to add the plate to the "Manual Reports" alert list for use in the field. **NOTE**: All manual entries are cleared with each End Shift

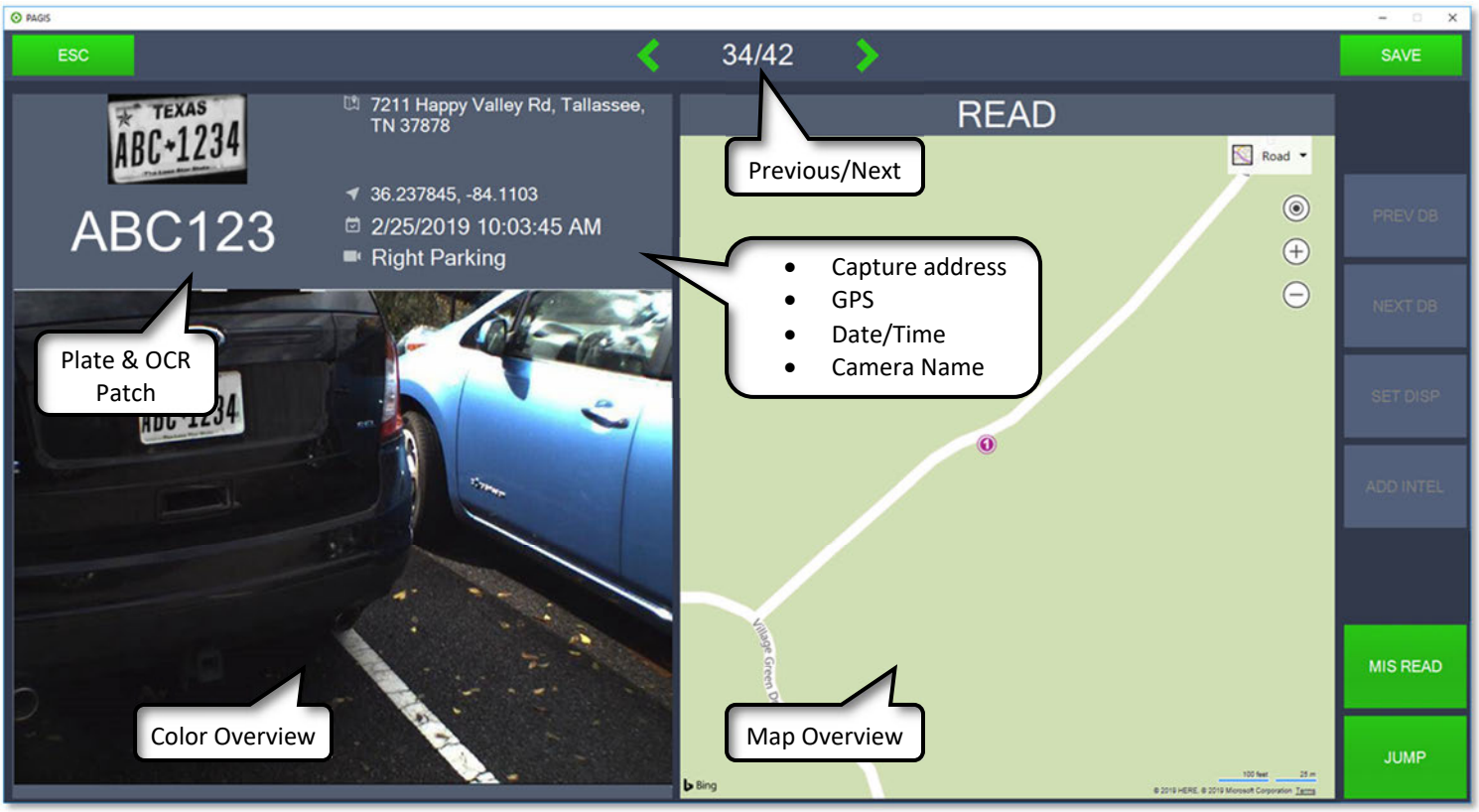
ESC: The Escape button allows the user to exit to the Main/ Live View screen.

2.8.2 Searching Locally Stored Reads and Hits

As mentioned previously, this search function allows users to find reads and hits directly from their recent patrols using the search field and the Reads button. These searches pull only the reads and hits locally gathered/stored since the last time the user completed an End Shift. **NOTE**: The search results are specific to each Windows User Profile and do NOT pull images from the BOSS server.

2.8.2.1 Searching for a Match

- From the Search field, users may enter a plate (or partial plate with wildcards) and then click the **READS** button.
- Results are displayed with the data gathered at the time the read was taken (See example below).
- Each result should display the infrared (IR) image of the plate as well as the color overlay of the vehicle for review.
- Each result shows the GPS data, Closest address point, Time and Date, and the Camera that read the plate.
- If there are multiple results, the user can cycle through them by clicking the left and right navigation arrows.



2.8.3 Wild Card Symbols

The use of wild card symbols in the Search box allows greater flexibility for the user, but may return a larger set of results.

- Wild card searches performed using the asterisk (*) designates an unknown number of characters.
- Wild card searches performed using the underscore (_) indicates a single missing or unknown character.
- Searches can be performed using one, both or no wild card symbols.

Example: The officer received an alert from Dispatch looking for a vehicle plate containing the letter J and the number 8 separated by one character. Because the officer doesn't know how many characters there are before or after the J and 8, he enters *J_8* in the search box to review all possible matches of J and 8 separated by only one digit.

2905

2.8.4 Manually Adding a Plate to PAGIS

PAGIS allows users to manually add a plate of interest directly into the software as needed. Once saved, these entries are stored as part of the Manual Reports alert list and work just like any other Hotlist synchronized from the BOSS server.
NOTE: These additions are designed to be temporary and are cleared from the software with each End Shift.

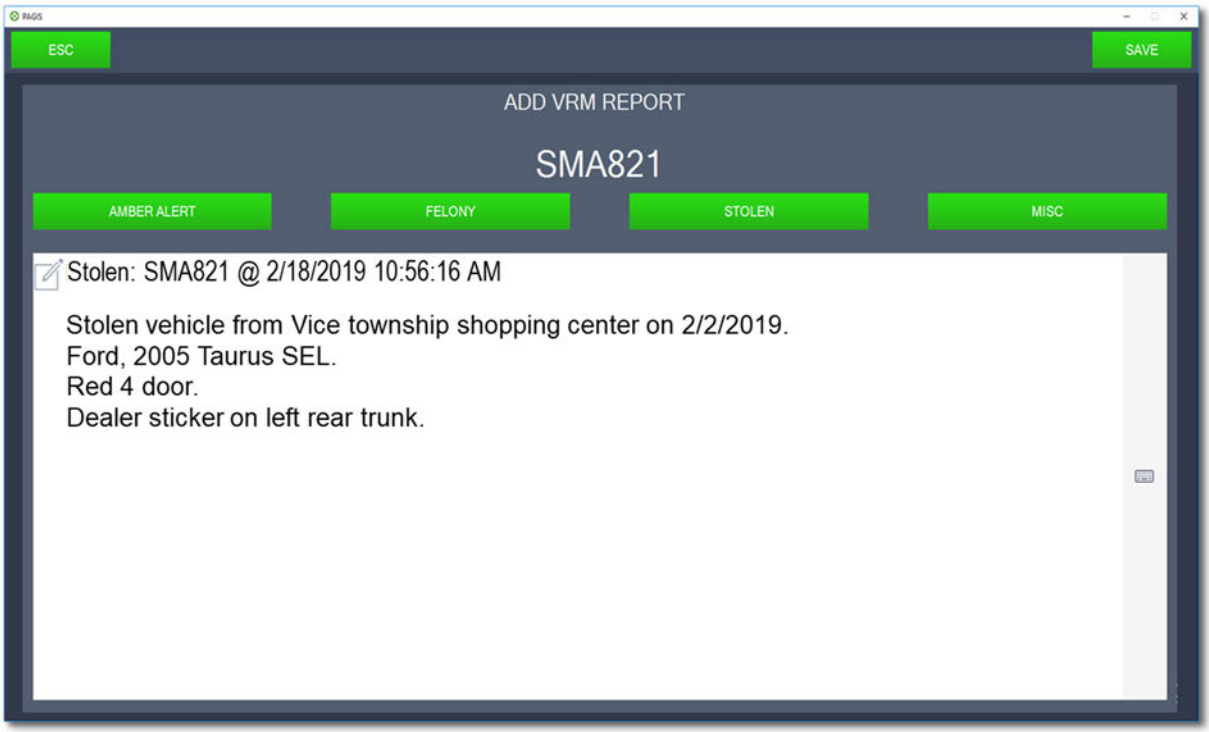
2.8.4.1 ADD VLP Query

Before an entry is added to the Manual Reports Hotlist in PAGIS, the software searches all stored databases for a match. If a match occurs, a message will display under the search box showing which Hotlist(s) it has been found in. If the VLP query does not return a match, the "ADD VRM REPORT" screen appears.



2.8.4.2 ADD VRM Report Screen

If the desired plate does not already reside in another Hotlist, the ADD VRM Report Screen becomes accessible to the user.



1. From the Search Entry Screen, enter the desired plate to add.
2. Click the ADD VLP button. If no match is found on any other hotlist, the "Add VRM Report" screen will appear.
3. Click to select the applicable alert type (AMBER ALERT , FELONY , STOLEN , or MISC)
4. Either leave the default information or add additional detail.
5. Click Save at the top right to add the plate to the Manual Entries Hotlist

2.9 The Review Screen

PAGIS allows users to review all locally stored data from one easy location. Clicking the Review icon from the Main Screen launches Review. This screen is divided into the Summary View Chart and sub-section navigation buttons to the right.



2.9.1 Summary Review Section

The Summary View Chart is divided into five categories and allows a user to review the information collected during their shift at a glance.

Total Reads: Shows the total number of Reads/Hits synced to BOSS and the total number of reads captured during the shift.
Reads: Shows the total number of reads synced to BOSS and the total number of reads captured during the shift.
Hits: Shows the total number of hits synced to BOSS and the total number captured during the shift.
Misreads: Shows the total number of reads marked as a "misread" synced to BOSS and the total marked during the shift.
Audits: Shows the total number of audits synced to BOSS and the total number of audits during the shift.
Targets: Shows only the number of targets downloaded from BOSS.
(NOTE: The Sync value will always be zero for customers using Disk Sync mode/Client Tools.)

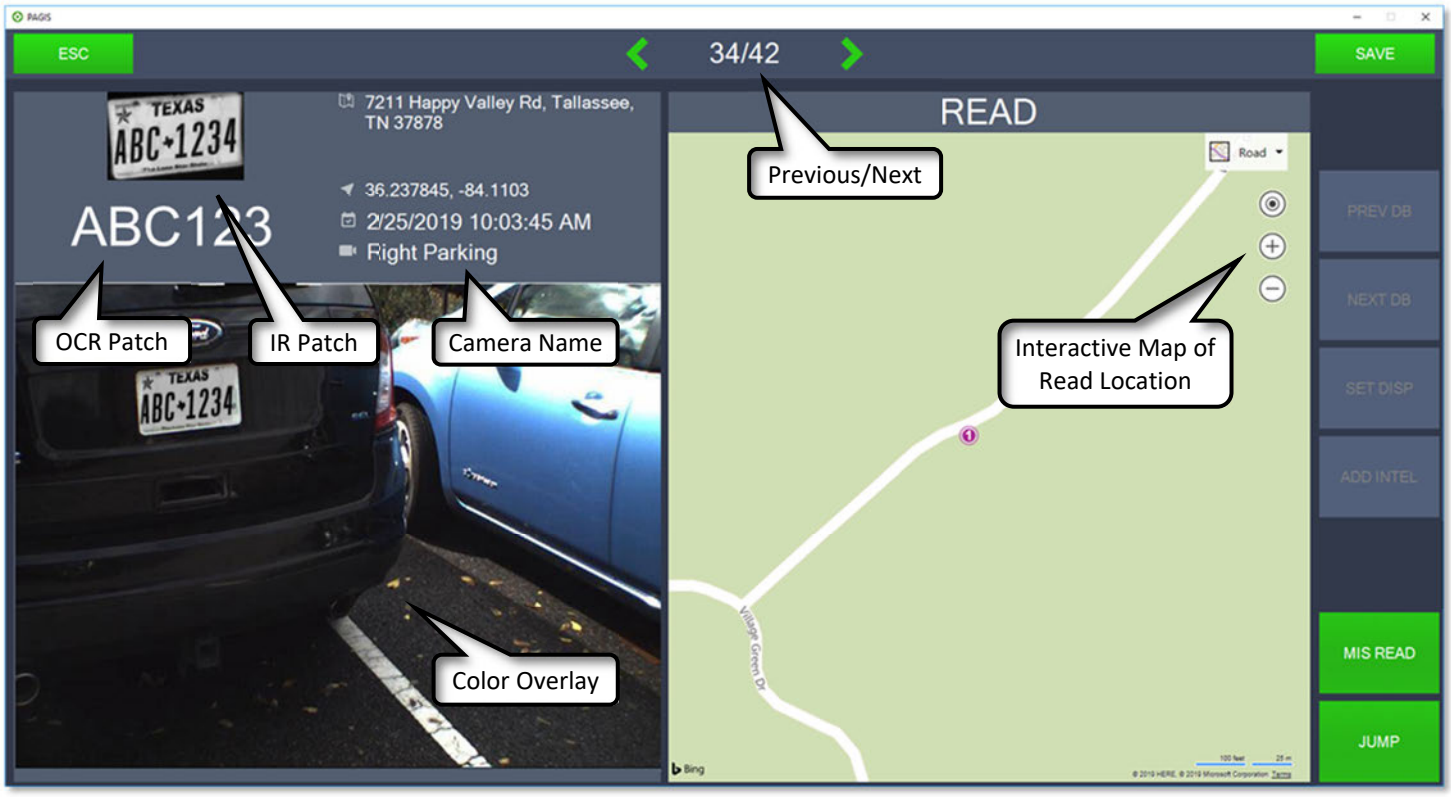
2.9.2 Review Navigation Buttons

The navigation buttons allow the user to review specific sets of information gathered during the shift.

Reads: Review all plate detections that have occurred since the last End Shift synchronization.
Hits: Review the hit alerts for Vehicle License Plate (VLP) reads that matched a Hotlist.
Misreads: Review reads and/or hits that have been manually flagged during the shift as misreads, where the plate number in the image does not match the OCR interpretation of the plate (e.g., a letter O misread as a Q or zero).
Audits: Review failed and successful logons, any manual data entered during the shift, pictures taken and all manual license plate searches.
Targets: Review targets that have been synchronized/downloaded from Boss.
Databases: Review all the Hotlists currently distributed to this PAGIS laptop/MDC.
Esc: Returns the user to the previous screen.

2.9.3 Reads

From the Main Screen, the user can review his or her accumulated Reads (those gathered since the last End Shift was completed) by clicking on the Review icon and then selecting the Reads Navigation button. The Read Review Screen is divided into two main sections. The left side displays the information gathered at the time of the read and the right side displays an interactive map of the GPS location.



NOTE: Buttons that are greyed out indicate options that are not available in the current view. For example, the Reads and Hits review screens share the same layout but different on-screen options.

2.9.3.1 Reads Result Screen Navigation Buttons



Read Count: The left number is the current record. The right number is the total available for review.

Next/Previous button: The arrows on either side of the read count allow the user to navigate back and forth to review reads/results.



MisRead button: When the button is green it indicates the record has NOT been edited as a Misread by a user. Once a Misread is saved, this button will turn grey and the record title will update.



Jump button: Allows the user to "jump" to a specific record without the need to navigate one record at a time using the Next/Previous buttons.



Save button: Apply any changes/edits and return to the Main Screen.



Escape button: Returns the user to the Main Screen.

2.9.3.2 Interactive Buttons – Reads Screen

From the Reads Review, the user can interact with the following:

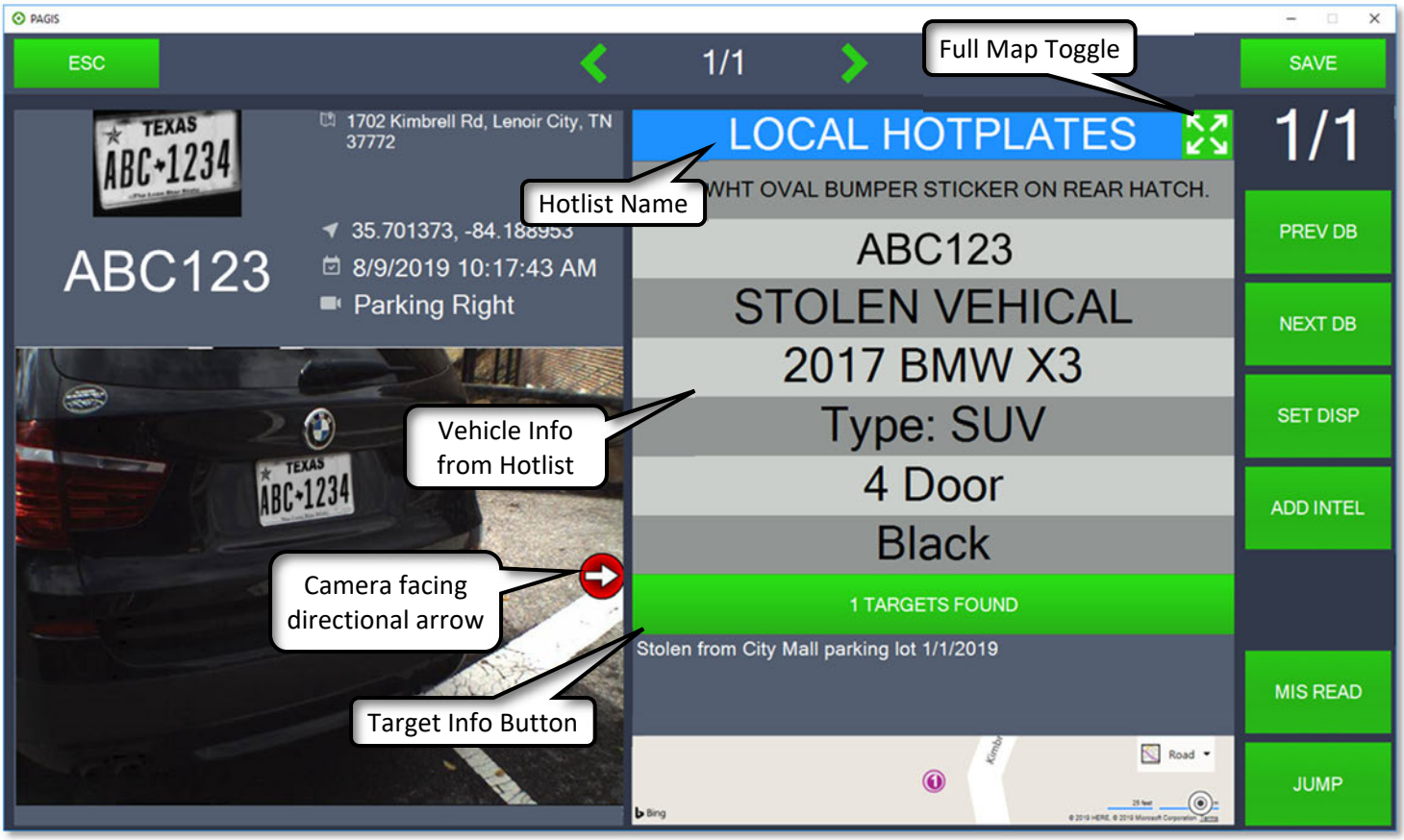
- IR Patch: The user can click on the IR "Patch" plate image to open a full-screen view.
- OCR Patch: The user can click on the OCR "Patch" image to edit the license plate number if necessary/Misread.
- Color OV Image: The user can click on the color image to open a full-screen view.
- Map: The user can manipulate the interactive map of the read location (Map Type, Scroll, and Zoom).

2908

2.9.4 Hits

Users can manually access the Hits Section by first selecting the Review icon from the Live View Screen and then clicking the Hits Button. The Hits Screen is also divided into two main sections. The left side displays the information gathered from the ALPR equipment during the read. And the right side displays the information provided by the associated alert list.

NOTE: Each time a VLP matches a Database value (a license plate read by the system matches a Hotlist entry), PAGIS plays an audible tone and automatically displays the Hit Screen to alert the user.



2.9.4.1 Hit Screen Attributes

Hit Count and Navigation Buttons: Displays the total Hit count as well as the Next/Previous navigation buttons.

IR Patch Image: A thumbnail image of the license plate from the IR camera.

OCR Text: The character string the OCR engine generated from the current plate.

GPS Location: The GPS coordinates at the time of the hit. (If a GPS device is not attached, the Lat/Long is displayed as 0,0).

Date and Timestamp: The date and time when the read/hit was captured.

Overview Image: The overview image of the vehicle from the Color Camera. (**NOTE**: Color images require visible light)

Camera Name: The name of the camera that captured the read ("Right Parking" in the screenshot).

Hotlist Name: This is the name of the Hotlist or "Database" where the plate was matched.

Target Button: When available, this indicates a person of interest is associated with the Hit and opens the Targets Screen.

Vehicle Information: The area of grey bars will display the related vehicle information from the Hotlist. Any information added manually by the user will appear in the Text Box near the bottom of the screen.

Interactive Map: Shows the location the Hit took place. Users can access full-screen view by clicking the map or the toggle .

2909

2.9.4.2 Hit Screen Function Buttons



The Hit Count Indicator: shows how many Hotlists the current Hit has registered against.



Previous DB button: This button moves the user to the previous Database/Hotlist that produced a Hit.



Next DB button: Pressing this button moves the user to the next Database/Hotlist that produced a Hit.



The Set Disposition button: prompts the user to report the disposition of the hit by selecting one of the approved codes assigned in BOSS by the Administrator.



The Add Intel button: allows the user to add additional information regarding the current Hit.



The Misread button: allows the user to flag the Hit as a misread.



The Jump button: Allows the user to "jump" to a specific Hit instead of navigating one at a time.

2.9.4.3 Interactive Buttons – Hits Screen

- IR Patch: The user can click on the IR "Patch" image to open a full-screen view.
- OCR Patch: The user can click on the OCR "Patch" image to edit the license plate number if necessary/Misread.
- Target Button: Shows associated person(s) of interest and opens the Targets Screen.
- Color OV Image: The user can click on the color image to open a full-screen view.
- Map: The user can manipulate the interactive map of the read location (Map Type, Scroll, and Zoom).

2.9.4.4 Set Disposition – Additional Detail

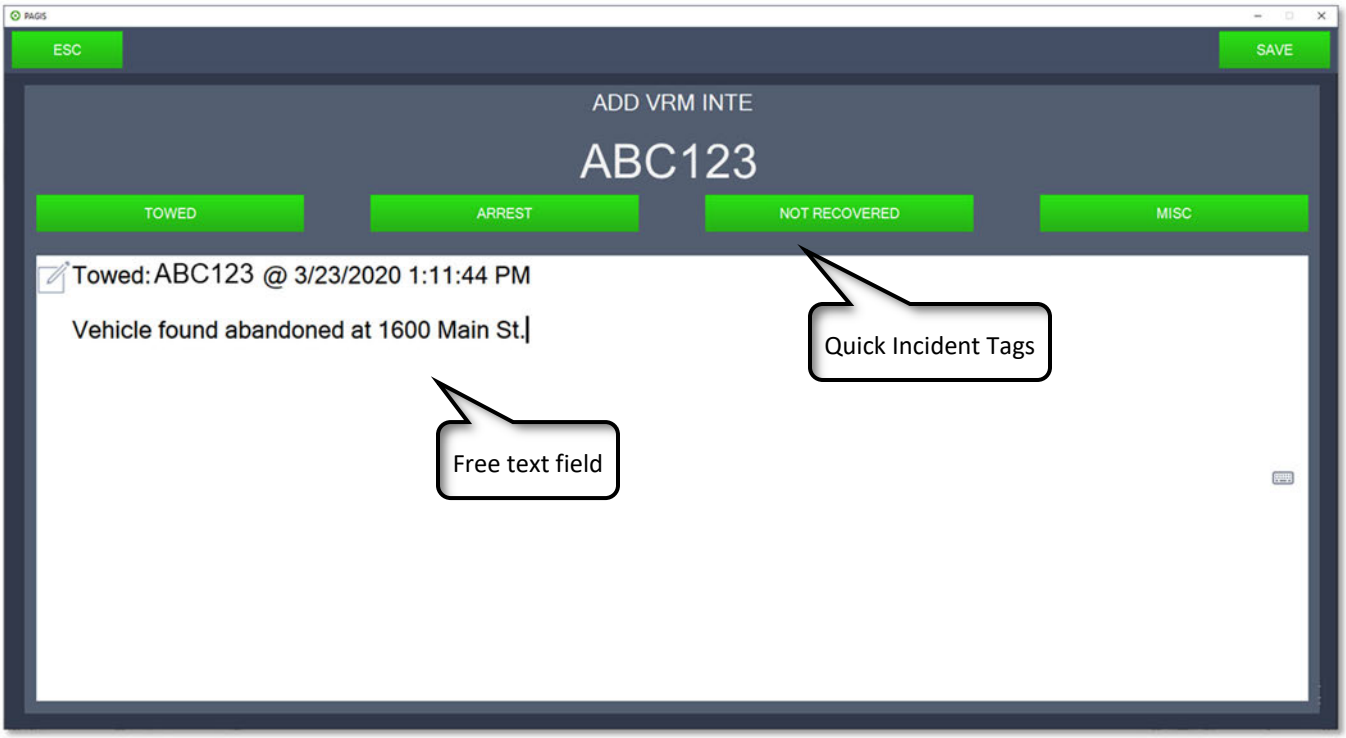


PAGIS allows for additional information to be added to a record in the form of a Disposition. Once Hits are flagged with a disposition code, the Agency is capable of running a "Reads Statistics by Disposition Report" in BOSS. Thus, providing valuable metrics and understanding to leadership in regard to their ALPR Enterprise.

When the "Set Disp" button is selected, the user is prompted to choose from a list of predefined values set by the Agency/BOSS Administrator. Once a disposition is selected and Saved, the disposition is reported to BOSS and will also show up in the Hits Review Screen text box in PAGIS on the next alert notification.

2.9.4.5 Add Intel – Additional Detail

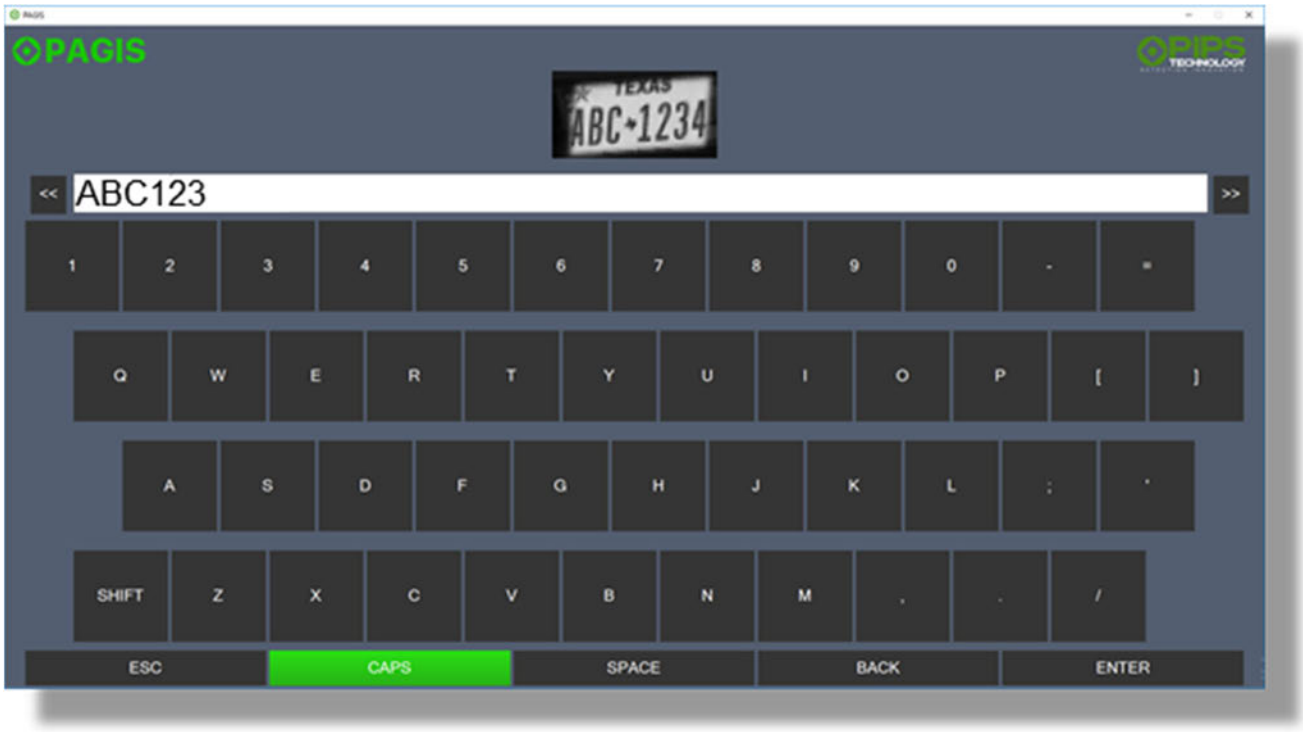
The Add Intel button launches the Intel screen. The user is prompted to assign one of four values: Towed, Arrest, Not Recovered, and Misc. by clicking the associated button at the top of the screen. The user may also enter additional detail regarding the license plate/vehicle. After clicking the Save button, the intel will now appear in the Hits Screen text box.



2.9.5 Misreads

PAGIS allows the user to mark Reads and Hits with incorrect OCR translations as a Misread. This is most commonly done by Agencies for Hits only as users typically don't have time to review every single Read from their shift. Once an errant Hit is corrected, the system updates the record to show it as a Misread and thus improves Agency Hit Reporting.

Correcting a plate read can be accomplished by clicking on the "OCR Patch" in either the Hits or Reads review screen. When the user clicks on the OCR Patch, the OCR Edit Screen opens and allows the user to update the Vehicle License Plate (VLP) data.



2911

2.9.5.1 Marking a Record as a Misread:

The user can mark a record as a Misread from both Reads or Hits Review Screen. Each user can either simply flag the record as a Misread or update the OCR Patch information. **NOTE**: This ability is only available until the user has performed an End Shift function.

Manually Flagging a Read or Hit as a Misread:

1. Navigate to either the Reads or Hits Review Screen
2. Click on the Misread button on the Right
3. Click Save
4. Take note that the record title has now changed from “Read” to “Misread”

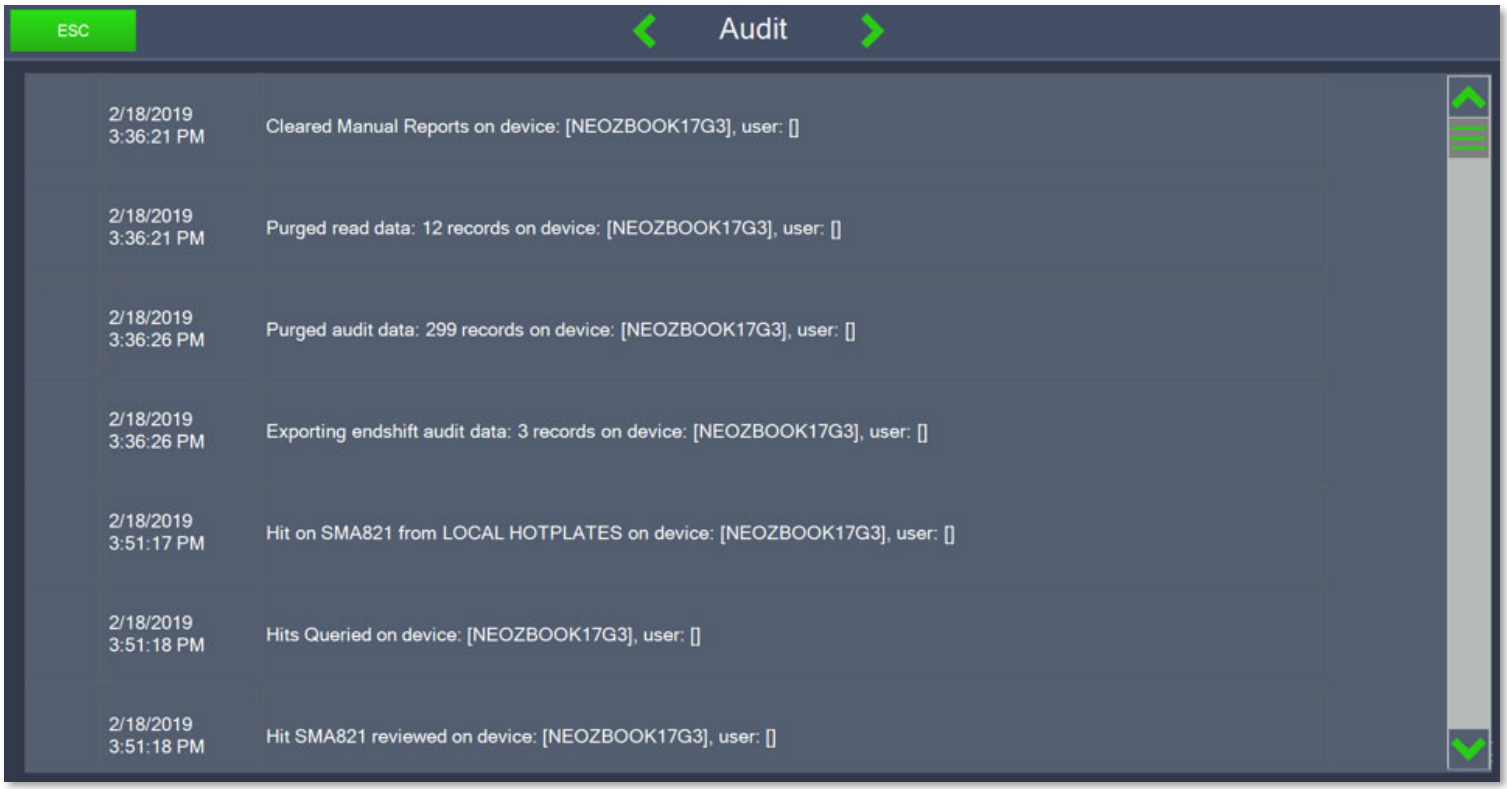
Updating the Read/Hit OCR Patch:

1. Navigate to either the Reads or Hits Review Screen
2. Click on the OCR Patch (Text just under the IR Plate Image)
3. Use the keyboard or on-screen keypad to update the Vehicle License Plate Number
4. Click the Enter Button to Save the changes (and exit back to the Review Screen)
5. When the user saves the changes to the OCR Patch, the record (Read/Hit) is automatically flagged as a Misread

2.9.6 Audits

PAGIS logs both user and key system activity during each use of the software. The audit log captures various information like Read searches, synchronizations, hits, and user login attempts. The Audit Report is viewed in PAGIS by navigating to the Review section and selecting “AUDITS”.

NOTE: Performing an End Shift or syncing the database clears the current log.



2.9.7 Targets

PAGIS has the ability to display information regarding Persons of Interest in response to a Hit alert. Targets are created by BOSS/Hotlist Administrators, and typically provide detailed information about owners of a registered vehicles. When configured, Target data is always linked to unique VLP data (a specific License Plate). If PAGIS registers a Hit on a Plate with a target ID, the Target Information Button is displayed in the Hit Alert window and allows the user to access the Target Screen.



2.9.7.1 The Targets Screen

When a PAGIS user clicks the Target Information Button from a Hit Alert, the Targets Screen opens. This screen displays the information from the BOSS server about the Person(s) of Interest matched to the Hit (license plate).



2.9.7.2 Targets Screen Navigation Buttons

If a Hit alert has more than one Target associated with it, the PAGIS user can navigate all Target information with the buttons described below:



Target Count: The left number is the current record. The right number is the total available for review.



Next/Previous button: Arrows on either side of the target count allow the user to navigate back and forth to review the various targets.



Jump button: Allows the user to "jump" to a specific record without the need to navigate one record at a time using the Next/Previous buttons.



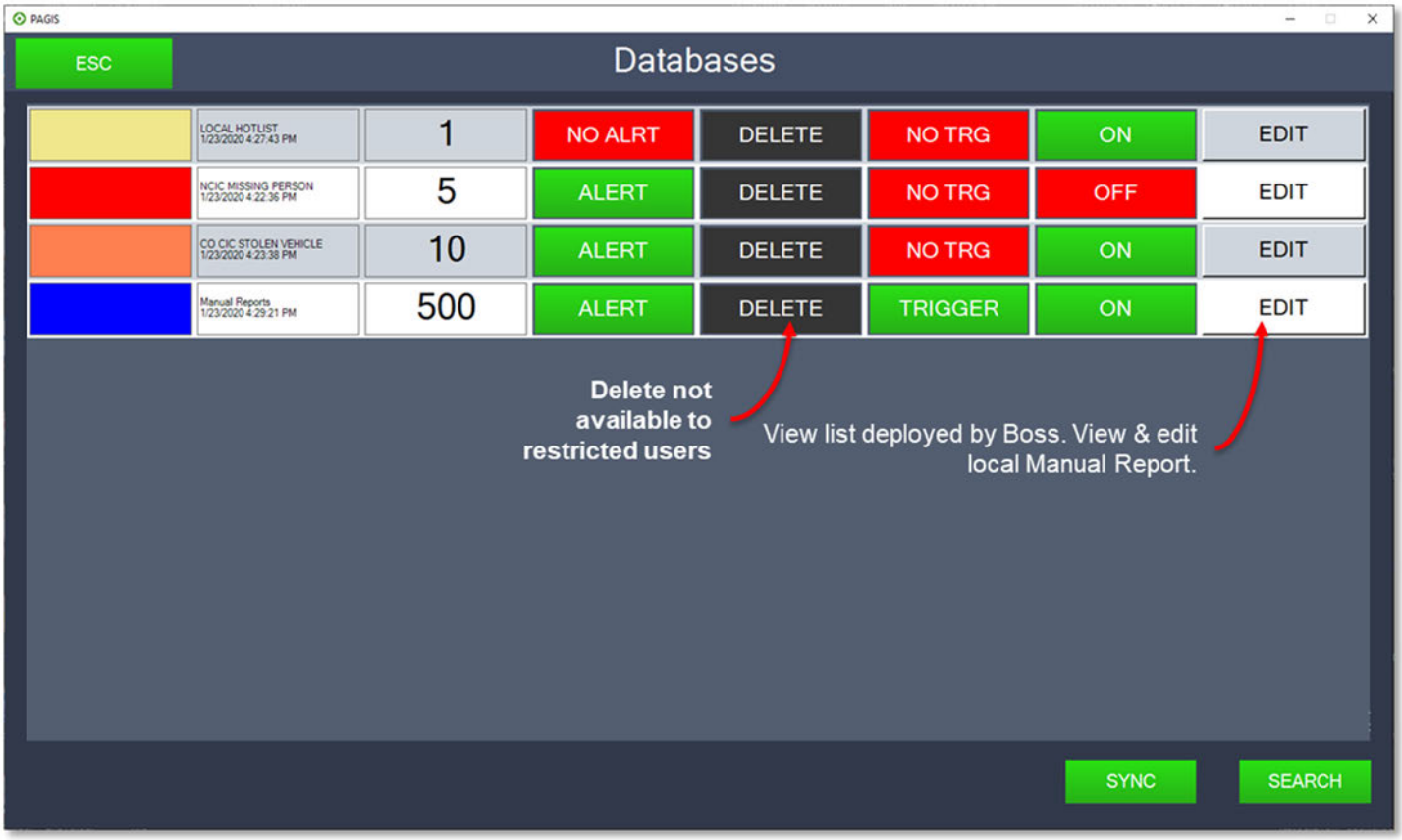
Close button: Returns the user to the previous screen.

2914

2.9.8 Databases

Users can review Hotlists in PAGIS by navigating to the Review section and selecting “DATABASES” on the right. From the Databases Screen, users can toggle Hotlists functions On and Off based on their rights.

NOTE: User rights and Hotlist attributes are configured in BOSS.



2.9.8.1 Databases Screen Functions

Hotlist Color Code: The color attributed to each Hotlist by the BOSS Administrator.

Hotlist Name: The name of the Hotlist given by the BOSS Administrator. Also shows the time/date of the last synchronization.

Hotlist Priority: The priority of the Hotlist assigned by the BOSS Administrator. The lower the number between 1 and 999, the higher the priority. If a plate resides on multiple Hotlists, the list with the higher priority will be displayed first.

Alert Button: Toggles audible alerts On and Off for each Hotlist until the next synchronization.

Delete Button: Based on user rights, allows the user to temporarily delete a Hotlist from PAGIS until the next synchronization. To delete a hotlist, the user must click the button twice (it turns green and then deletes the list).

Trigger Button: Toggles external triggers On and Off. An example of an external trigger is a light bar.

On/Off Button: Disables and enables each Hotlist (each Hotlist is set to On by default).

Edit: View and edit localy created hotplates with a given hotlist, Hotlist/Hotplates deployed via BOSS can only be viewed.

NOTE: Hotlist settings altered in PAGIS will be reset to their default configuration during the next Sync or End Shift. The default configurations are assigned by the BOSS Server/Administrator.

2.9.8.2 Databases Screen Navigation Buttons

SYNC — **Sync button**: Synchronizes PAGIS with the BOSS server in order to update the Hotlists.

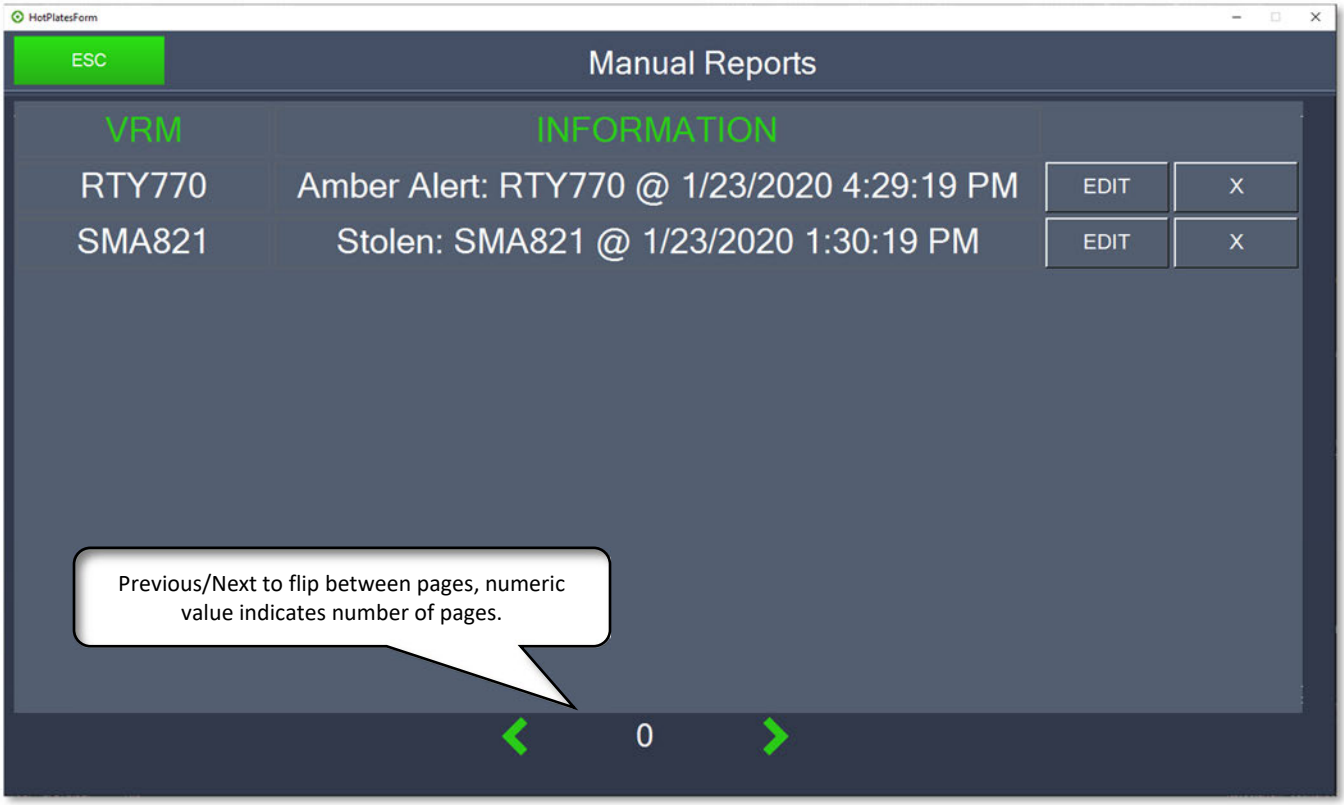
SEARCH — **Search button**: Open the Search Entry Screen (See section 2.8 for more information).

2915

2.9.8.3 Databases Edit- “Manual Reports”

Editing Hotlist has two function based on origin of hotlist.

- Hotlist deployed to PAGIS via BOSS cannot be edited, only the hotplates list can be viewed. Editing/updates are indented to be managed via BOSS.
- Hotlist created in PAGIS, i.e. “Manual Reports” can be managed by PAGIS users, allowing for changes or deletion of the hotplates contained within the hotlist.



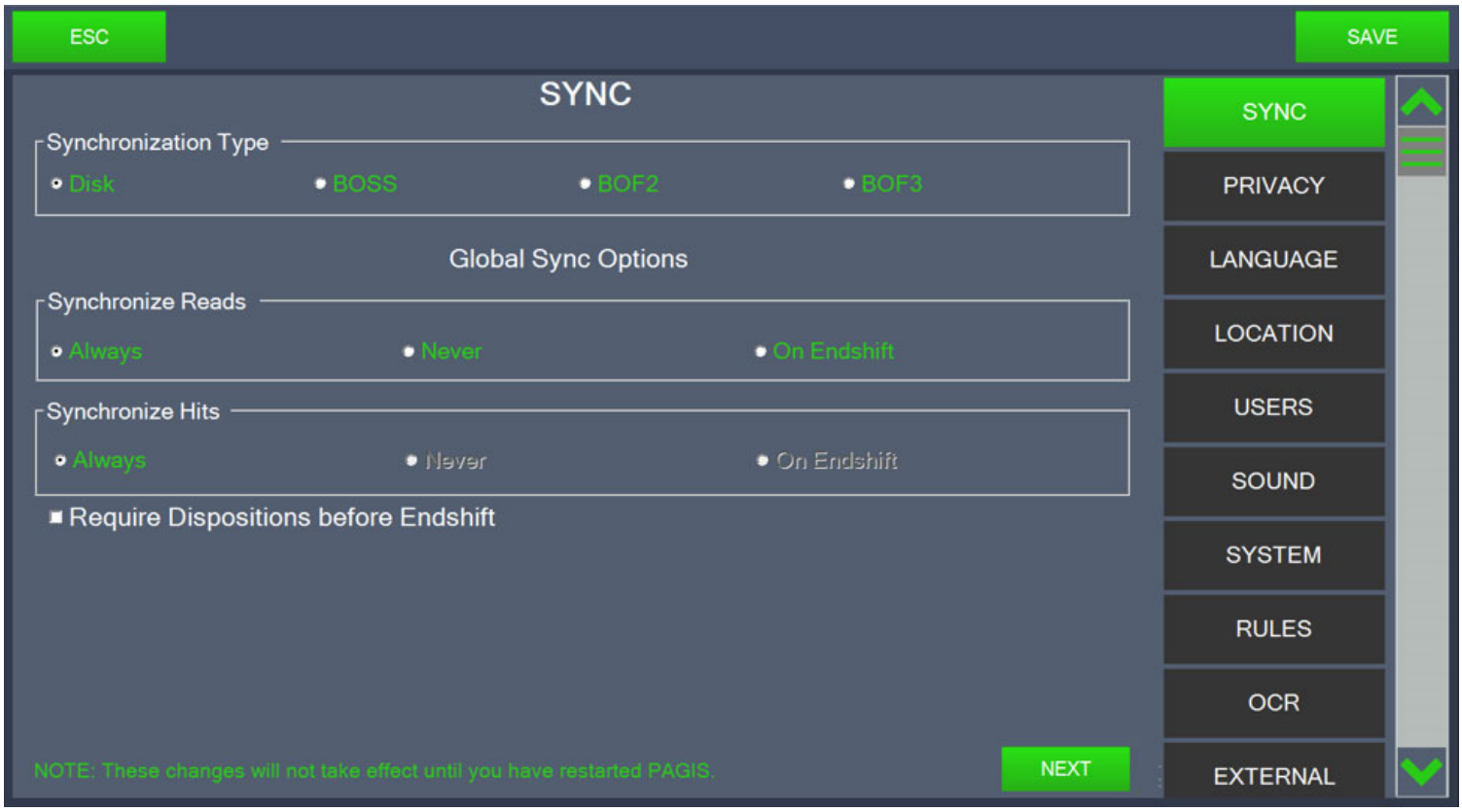
EDIT Button: Make changes to the indicustly hotplate information including licanse plate nuamber.
X Button: Remove indivualy hotlist from hotlist.
Previous/Next Button: Scroll thought lising of hotplates contaned within the hotlist. The numeric value indicates the number of pages.

ADMIN SETTINGS

The Settings Menu is the central location for configuring PAGIS Software functions endpoint by endpoint. Users with Admin level rights in PAGIS can see and click on the Settings Button from the Live View Screen. Launching Settings opens the menu to the Sync Options Screen by default. **NOTE**: Users without Admin level access will not see this icon on the Live View Screen.

3.1 Sync Options Screen

As mentioned previously in sections 2.4 and 2.5, PAGIS uses various sync options to store, update, and synchronize ALPR data to and from the BOSS server. On the Sync Screen, Administrators configure the synchronization method and options.
NOTE: Configuration changes will not take effect until they are saved and the PAGIS Software has been restarted.



3.1.1 Synchronization Types

- **Disk**: Uses local storage of Sync files in conjuction with a USB flashdrive to manually Sync to and from BOSS.
- **BOSS**: Uses a wireless data network to Sync files to and from the BOSS server.
- **BOF2**: Used predominantly in Europe (see regional guide for support).
- **BOF3**: Used predominantly in Europe (see regional guide for support).

3.1.1.1 Synchronization to Disk (Local Storage)

Sync to Disk is a manual two-part process most commonly used with a USB Thumb drive. To use Begin Shift, the user accesses a centralized terminal (Ex. Patrol Room PC) to download the files from BOSS and then inserts the Thumb drive in the laptop to perform Begin Shift. At the end of the day, the user then Performs End Shift from the laptop/MDC connected to the Thumb drive and uploads those files to BOSS via the central terminal (See the "Client Tools" section of the BOSS Manual).
NOTE: From the Sync Menu, select "Disk" and click the Next button at the bottom to configure the drive location.

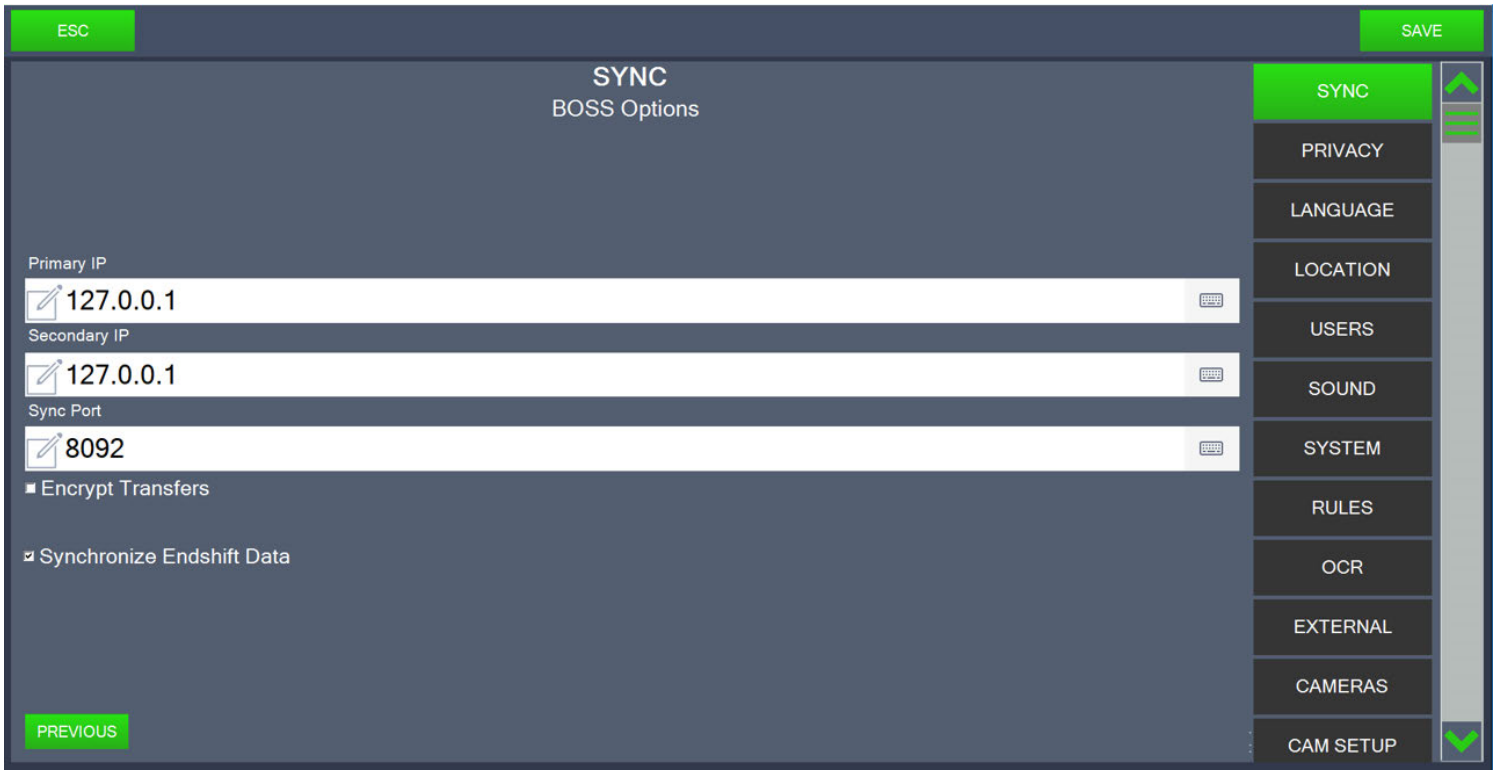


- **Delete Beginshift Data on Sync**: The sync folder on the Flash Drive is deleted once all Begin Shift data has been imported to PAGIS. This is on by default to help prevent false alerts.
- **Encrypt Endshift Data**: All uploaded End Shift data created in PAGIS is encrypted. This is off by default.
- **Copy Endshift Data on Sync**: If unchecked, no End Shift data will be transferred from PAGIS to the Drive location.
- **Keep Only Updated Databases**: Removes any Hotlists from PAGIS that were not updated during Begin Shift as "outdated". This is off by default.

Sync to Disk Setup:
In the text box, enter the drive path or letter to be used with Disk Sync. Folder name is not required as PAGIS creates the required folder(s). Once entered, select the desired options and then click the Previous button. Click Save to retain the settings.

3.1.1.2 Synchronization with BOSS

Sync to BOSS is a streamlined method for updating ALPR data to the field units and the server. Additionally, selecting this option enables the PAGIS auto-sync features that synchronize data throughout the shift without user involvement. However, this does require a stable data connection as well as some network configuration before it can be utilized.



Sync to BOSS Screen:

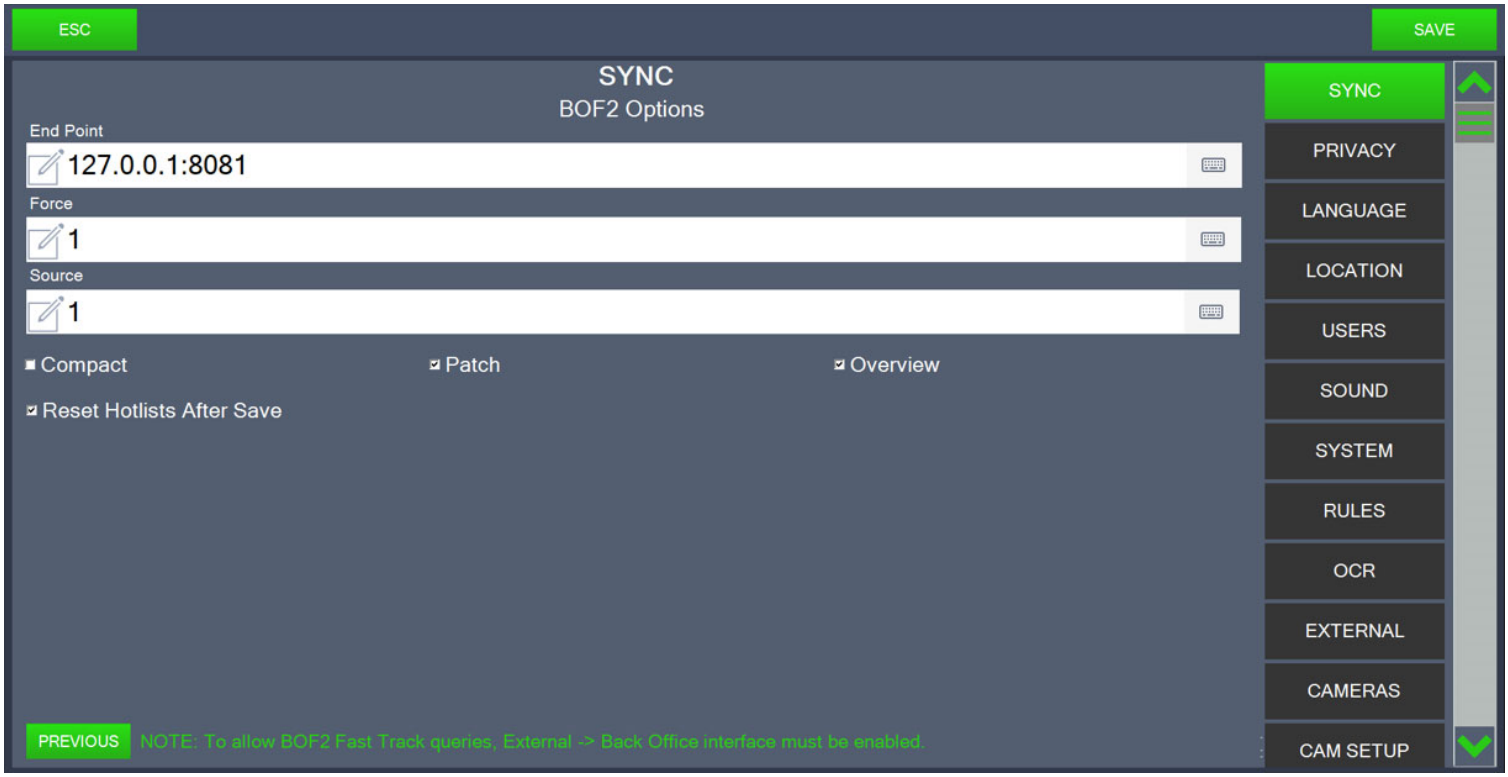
- **Primary IP**: The IP address of the BOSS server. This can also be the DNS name (**NOTE**: using DNS adds an additional failure point via the Domain Controllers and is not recommended as the best option).
- **Secondary IP**: Used for a secondary IP in cases where users switch from a cellular network to a Domain APN thus routing to BOSS from either an internal or external IP. This field can be left blank or with the primary IP as well.
- **Encrypt Transfers**: When enabled, data transfers to BOSS will be encrypted.
- **Synchronize Endshift Data**: On by default, this enables PAGIS to sync to BOSS when End Shift is performed by the user.

Sync to BOSS Prerequisites:
To establish the wireless sync to BOSS, the Agency Network Administrator will need to open TCP 8092 to the BOSS server as well as define the internal and/or external IP address(es).

Sync to BOSS Setup:
From the Sync Settings Menu, the Admin must select the BOSS option and click the Next button. Then s/he will update the Primary and Secondary IP fields as necessary and de/select any options. Once configured, click the Previous button and then click Save to retain the changes. (For more information on PAGIS Auto-Sync settings, refer to section 2.4.3)
NOTE: After synchronizing to BOSS, data is flagged in the database to prevent duplicate values on future synchronizations.

3.1.1.3 Sync to "Instation" (Formerly BOF2 and BOF3)

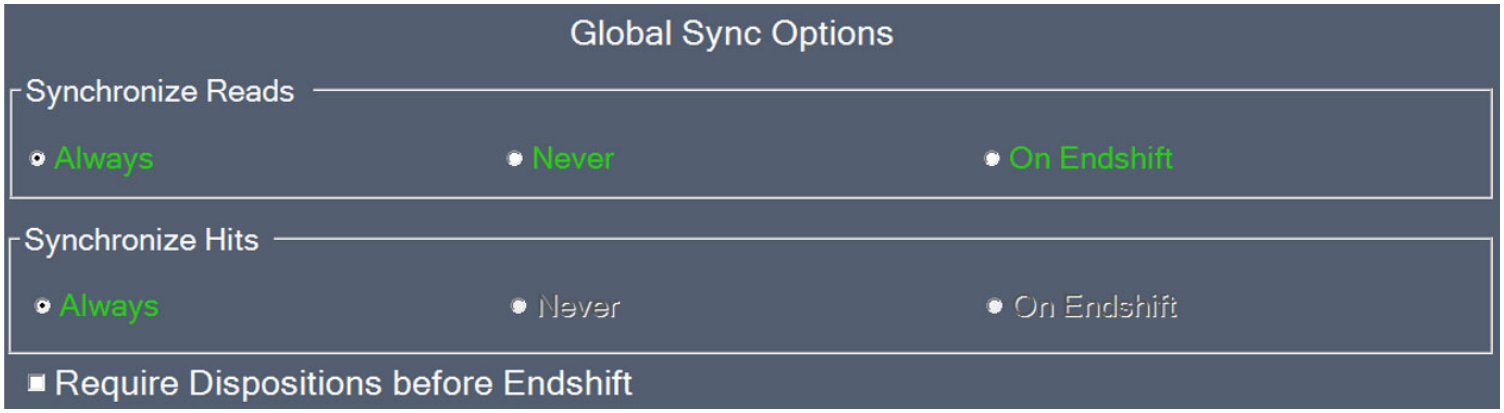
The Instation software was formerly known as BOF2 & BOF3 and was developed by Anite PLC. It is a web-based Back Office software suite used in European markets to provide similar features as the BOSS server and UI Client.
NOTE: These options are NOT used in the Domestic United States.



- **End Point**: The IP Address of the Instaion website. Format must be [IP Address:Port]
- **Force/Source**: Unique codes assigned to each police force.
- **Compact**: This option minimizes data transfer to Instation. Images will be deselected by default when in use.
- **Patch**: Refers to the image of the plate pulled from the read. This is on by default.
- **Overview**: Refers to the color overlay image from the read. This is on by default.
- **Reset Hotlists After Save**: When the software syncs to Instation, this will reset the hotlist tracking.

3.1.2 Global Sync Options

Global Sync settings control how PAGIS synchronizes ALPR data during Begin and End Shift cycles and applies to both manually launched synchronizations as well as Auto-Sync functions. The two sections are Synchronize Reads and Synchronize Hits.

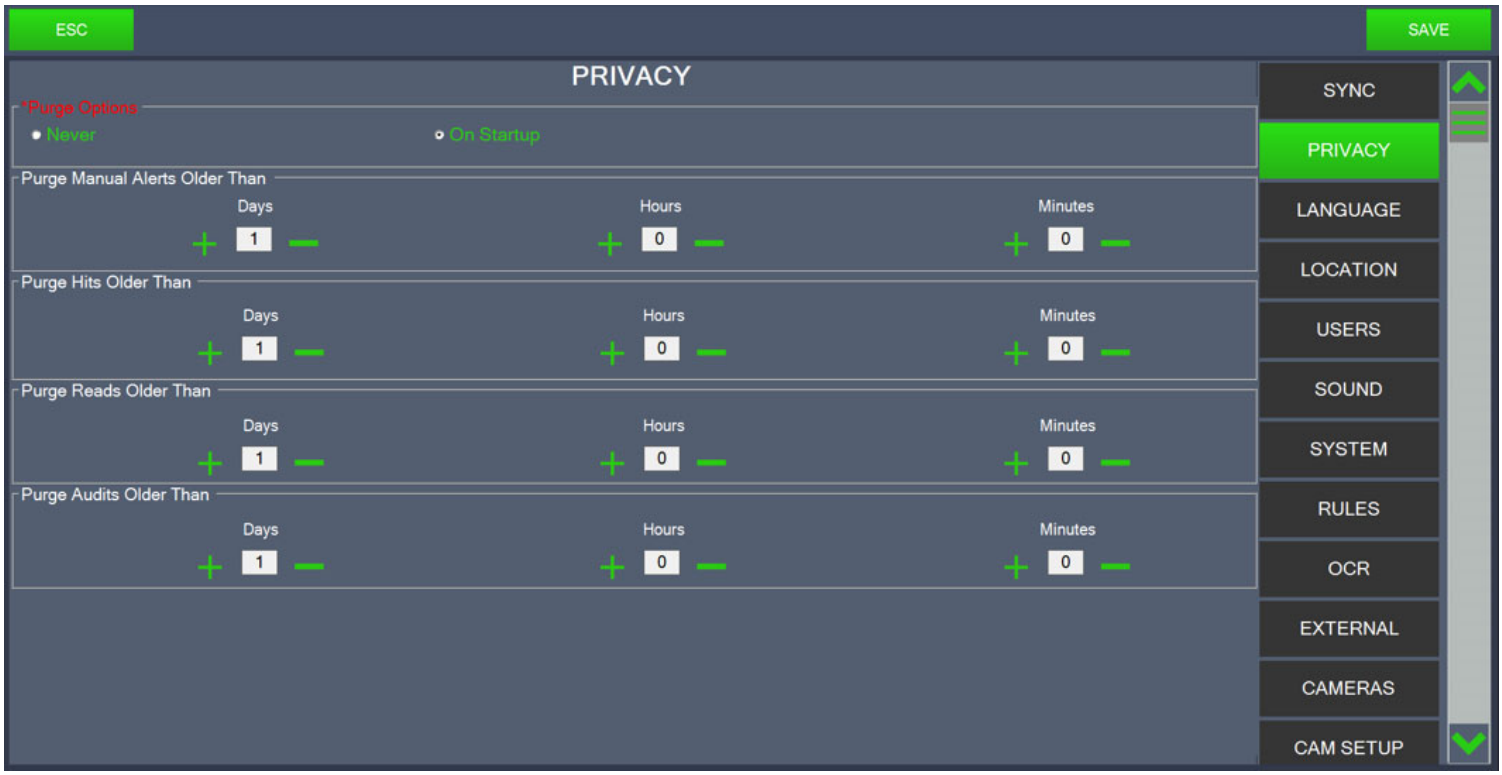


NOTE: All Hits are Reads, but not all Reads are Hits. A "hit" is a read that coincides with an Alert List. Due to this, the Options selected in the "Synchronize Reads" section dictate what options are available in the "Synchronize Hits" section. Unavailable options are greyed out.

- **Always**: Reads and Hits are synchronized to BOSS as close to real-time as the data network and PC processing allow.
- **Never:** The information gathered during the shift will be "sanitized" with each launch of End Shift. The corresponding data and images will NOT be sent to the BOSS server.
- **On End Shift**: Synchronization to BOSS will only occur when the user manually launches End Shift.
- **Require Dispositions before Endshift**: Requires the user to select a disposition code for each Hit registered in the PAGIS software since the last End Shift was completed before the Synchronization is processed.

3.2 PAGIS Privacy Settings (Local Data Retention)

Although most commonly configured in BOSS, the PAGIS Software allows the Admin to configure the data retention settings for the local endpoint by minutes, hours, or days. This feature ensures the data captured/stored on the MDC is sanitized by the software itself (this is important for customers without BOSS). **NOTE**: To enable the Privacy settings, the Admin must select the "On Startup" purge option and then set at least one value in each row. Rows left with all Zero will not be sanitized or purged.



- **Never**: Selected by default, this option disables the PAGIS privacy settings and uses only those set in BOSS.
- **On Startup**: This option must be selected in order to enable the PAGIS privacy settings. Once enabled, PAGIS looks to purge/sanitize the system each time it's launched or restarted.
- **Purge Manual Alerts Older Than**: Controls how frequently all of the Databases/Hotlists in PAGIS are purged. The purge rate is calculated from the timestamp of the Hotlist. Once the retention value is surpassed, the Hotlist is deleted. Hotlists distributed from BOSS will be re-downloaded on the next Sync.
- **Purge Hits Older Than**: Controls how frequently all Hits in PAGIS are purged. The purge rate is calculated from the timestamp of read. Once the retention value is surpassed, the Hit is removed the next time PAGIS is restarted.
- **Purge Reads Older Than**: Controls how frequently all Reads in PAGIS are purged. The purge rate is calculated from the timestamp of read. Once the retention value is surpassed, the Read is removed the next time PAGIS is restarted.
- **Purge Audits Older Than**: Controls how frequently all Audits in PAGIS are purged. The purge rate is calculated from the timestamp of audit. Once the retention value is surpassed, the audit is removed the next time PAGIS is restarted.

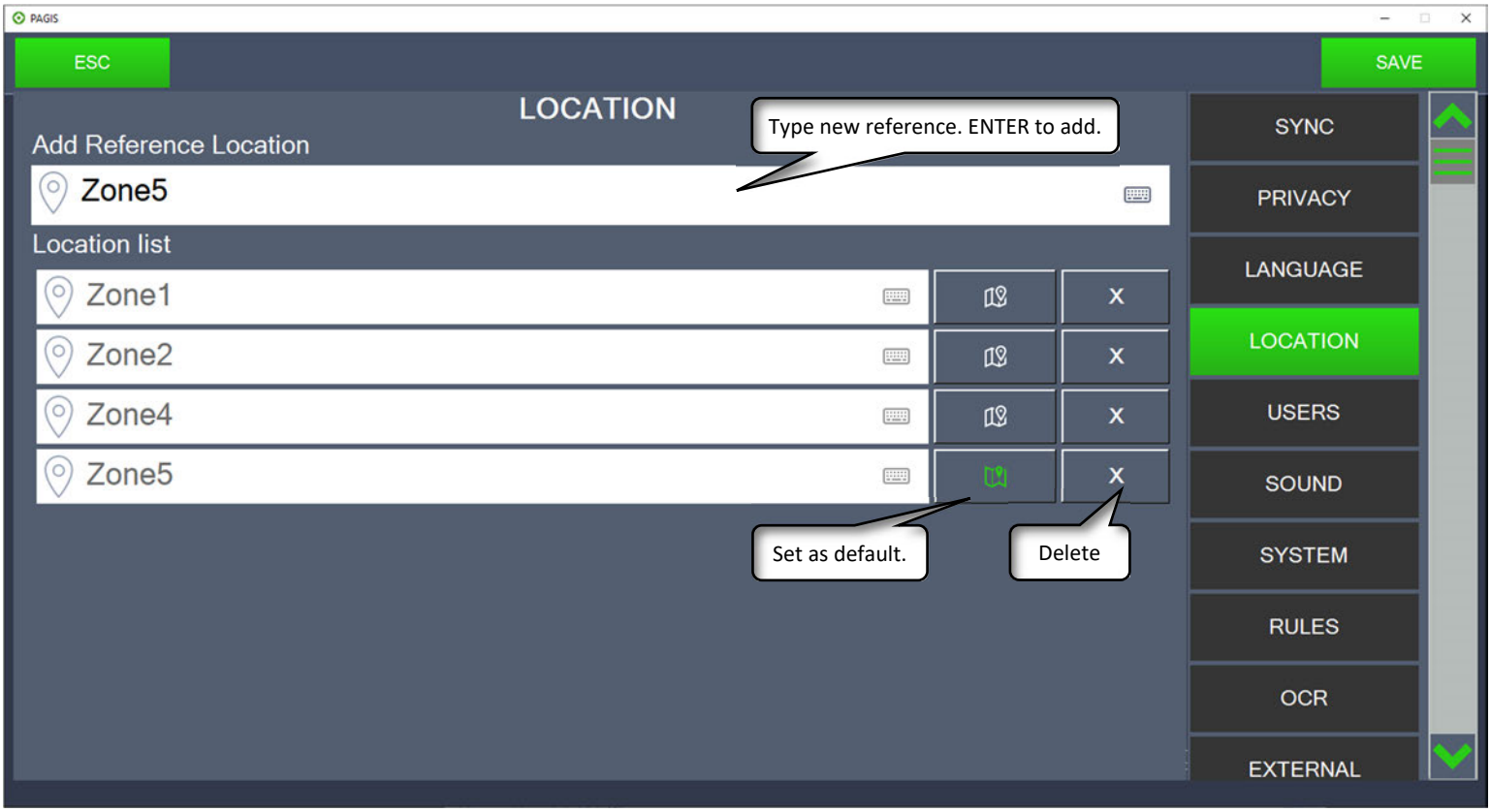
NOTE: Once the hits, reads, databases, or audits have been purged, they can no loner be viewed in the PAGIS software.

3.3 Language

The Language screen allows the Admin to change the language assignment used in the PAGIS Software. Available languages are listed in the drop-down list and are added during the installation process.

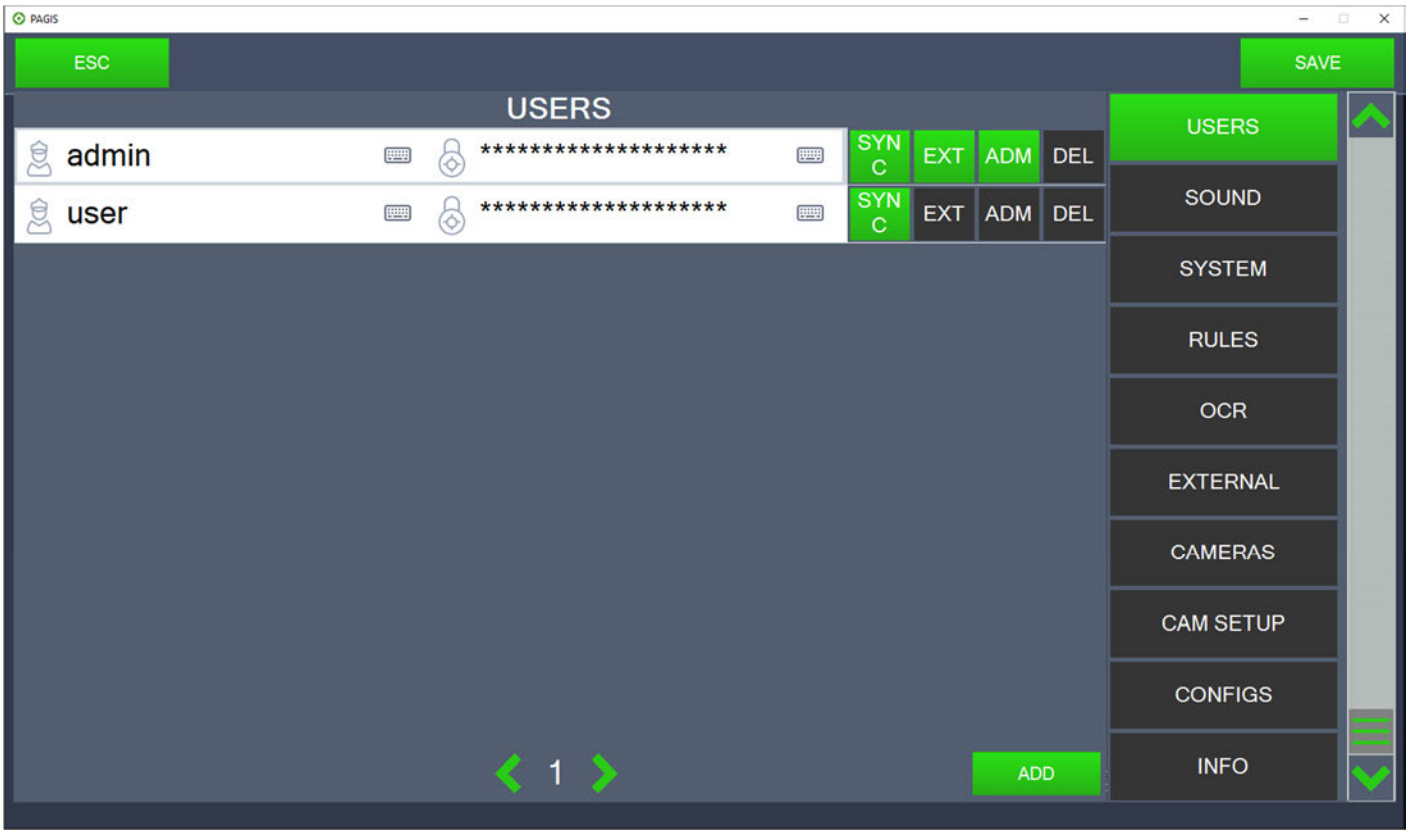
3.4 Location

Updates to the location field will auto-fill the “Reference” section of the PAGIS Login Screen. These are often used to specify a patrol region (Examples: “North Patrol” or “A2”). Once designated all reads/hits will show this designation. Muiltiple “Referance” location can be added, the available list can then be selected from the login screen.



3.5 Users 2022

User accounts, credentials, and rights are generally administered from BOSS and then distributed to the MDC. However, PAGIS does allow for Administrators to add and delete users as well as set their privileges directly from PAGIS.



NOTE: Adding user directly in PAGIS should be limited to customers not utilizing a BOSS server. User accounts created directly in PAGIS by customers with BOSS will be overwritten/removed during the next sync.

Adding a User in PAGIS:

1. From the Admin Screen, select the Users Button on the Right
2. Click the Add Button ADD
3. Enter the case sensitive username in the Username Field (max of 15 alphanumeric characters)
4. Enter the case sensitive password in the Password Field (max of 15 alphanumeric characters)
5. Select the User's privileges
6. Click the Save Button SAVE

3.5.1 User Privileges

These are the "rights" the new user will have in the PAGIS software (When selected, each button turns green).

SYNC — **Sync:** Allows users to synchronize data.

EXT — **External**: Allows the user to access external databases.

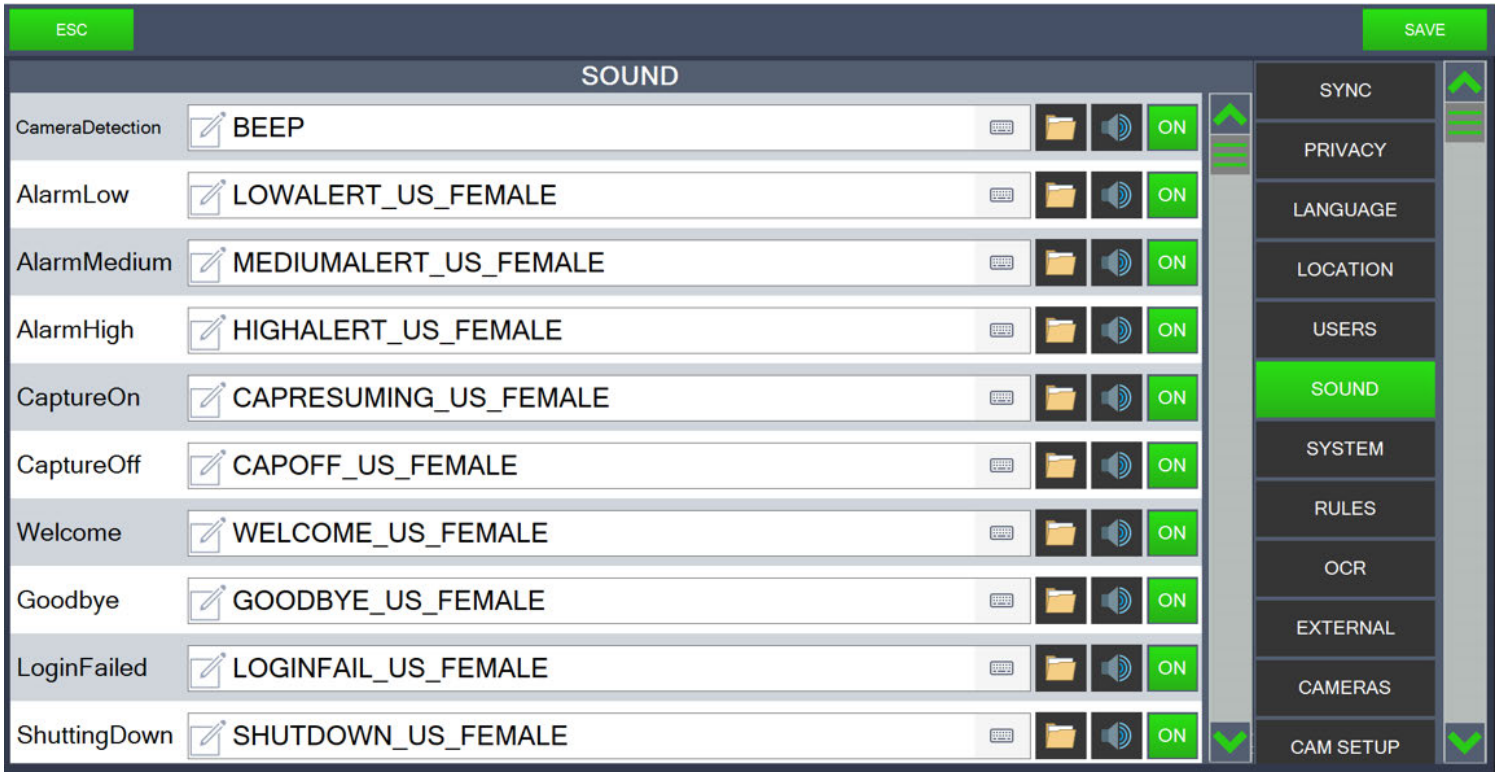
ADM — **Admin**: Provides the user Admin rights and allows him/her to configure the PAGIS Software.

DEL — **Delete**: Allows the Admin to delete a User from the list. Click once to select and the save button to delete.

NOTE: Creating a new user in PAGIS automatically deactivates the default user account settings (Section 2.1.1).

3.6 Sound 2023

Sounds in PAGIS mirror the user or software activity (Ex. Login, Audible alert from a “Hit”, and Logout) and are On by default. PAGIS Administrators can adjust the sounds from the available presets and/or load unique .wav files onto each MDC for custom use. **NOTE**: The default storage path is C:\Program Files (x86)\PIPS Technology, Inc\PAGIS2\sounds



3.6.1 Configuration Buttons

The sounds listed on the configuration screen can be altered or updated by PAGIS administrators using the buttons below. **NOTE**: Changes to any sounds must be saved before they can be played in PAGIS.



Click to browse to the sounds folder. This is used to select a new sound file.



Click to Test/Play the selected sound.



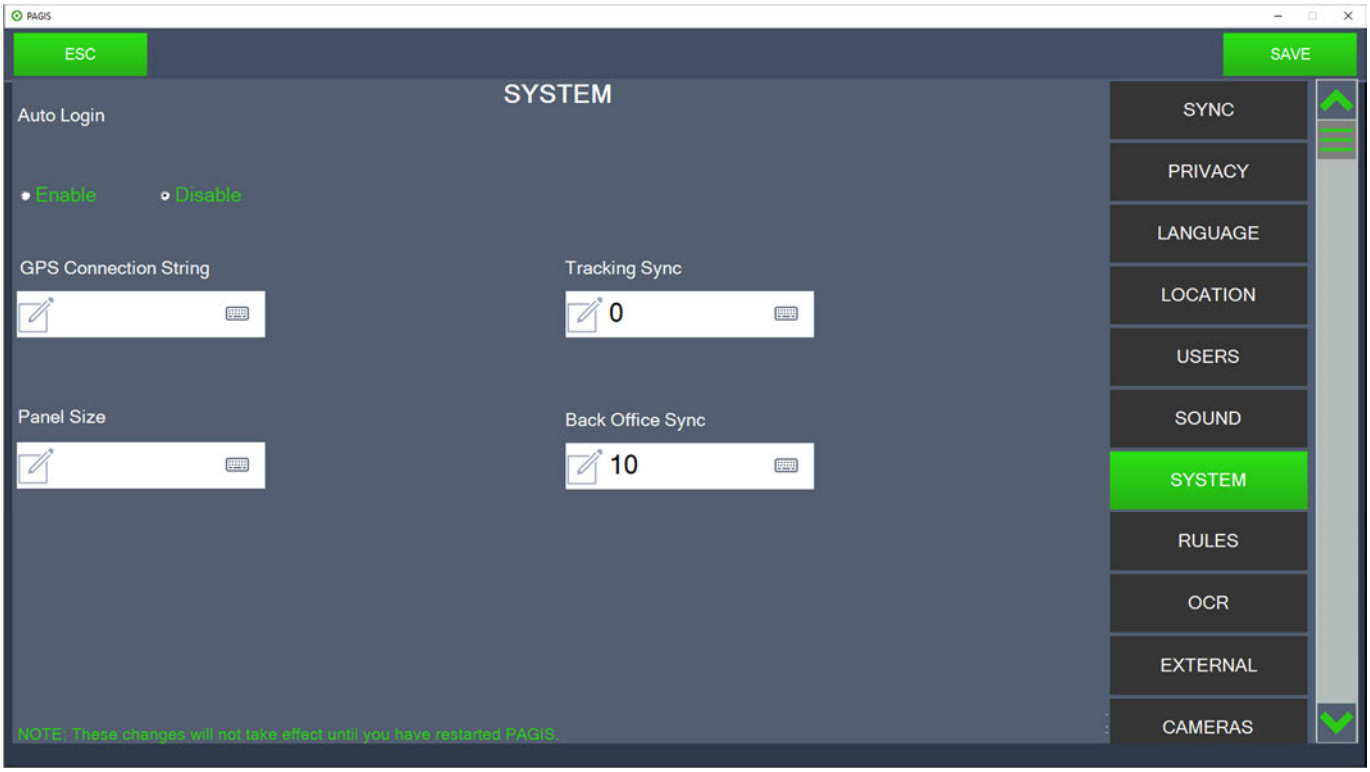
Shows the status of that sound. Click to turn each sound Off.



Shows the status of that sound. Click to turn each sound On.

3.7 System

The System screen determines external system connections. The primary external connection is the GPS antenna. The GPS connection string will accept TCP/IP ports or COM port designations. This section also contains control of the PAGIS "Auto Login" feature (which is set to Off by default).



- **Auto Login**: Enabling this feature will ignore existing user account information and login to PAGIS as the Admin. This feature is recommended only for unattended use (Speed-Trailer applications and Covert Drop and Go deployments).
- **GPS Connection String**: This value is utilized by PAGIS to acquire the GPS feed from its source. The default is traditionally either blank (no entry) or 6.
- **Tracking Sync**: Controls the sync intervals in (Sec.) that PAGIS communicates with BOSS4 to update tracking status. Default off=Zero, values can range from 1-9999. BOSS4 Back Office Software requiered for this feature.
- **Panel Size**: Controls the resolution of the color image displayed on the Live View Screen. By default this is blank as PAGIS controls the aspect ratio. However a PAGIS Admin can assign custom resolutions in WxL format (720x1024) to assist with non-standard dispalys.
- **Back Office Sync**: This setting controls the sync timing that PAGIS sends data back to BOSS3/BOSS4, Timing is in (Sec.), default is 10sec, values can range from 0-9999.

NOTE: All changes must be saved and will not take effect until PAGIS is restarted.

2925

3.8 Rules

Rules in PAGIS allow Administrators to force the software to process plate reads in specific ways. For example, in states that allow for both O and 0 (zero) on their license plates, a rule can be set to read any zero as an O and any O as a zero. This provides PAGIS greater flexibility to the standard OCR functions.



Adding a Rule to PAGIS:

1. Click the Add Button ADD
2. Enter the desired alphanumeric characters (Ex. 0 and O) into the text field
3. Click the Save Button SAVE at the top right of the screen

Deleting a Rule:

1. Locate the rule to be removed from PAGIS
2. Click the Delete Button DELETE to the right of the rule (It will turn green when selected)
3. Click the Save Button to complete the removal

3.8.1 Rules – Additional Clarifications

1. Rules are processed based on the first character entered. So in order to read any O as a zero, the Admin will need to add rule “O0”. And in order to read any zero as an O, a second rule must be entered as “0O”.
2. Rules are NOT designed to overhaul OCR function. Any consistently misread values should first be brought the attention of Neology Support for review. And only those cases where further adjustments to the OCR software are impossible would rules be recommended.
3. Adding rules to PAGIS will make it less likely to miss a Hit Alert. However, it will increase the number of Hit Notifications that require the Officer to visually confirm the OCR read (“IR Patch”) and the Hotlist Alert match.

2926

3.9 OCR

The OCR Section in PAGIS provides Administrators some additional options on how they would like PAGIS to process plate reads.



- **JPEG Images**: On by default, this forces PAGIS to use compressed .JPG images instead of the full resolution Bitmap images each time a read is taken. This settings minimizes data storage requirements and preserves MDC drive space.
- **Inverse Plates**: Off by default, this setting is only used in States where plates with light color lettering over a dark background are prevalent. Enabling this option increases processing load and should remian disabled unless required.
- **Square Plates**: Off by default, this setting adjusts the read area plates that are square instead of retangular.
- **Disable Duplicate Read**: On by default, this setting helps PAGIS prevent duplicate plate reads. If a VLP is read by more than one camera within a short period, the duplicate read is ignored. This minimizes data storage requirements and improves overall system metrics related to numbers of Hits and Reads.

NOTE: Once changes are made, the Admin must click the Save Button SAVE button in the upper right corner to retain them.

2927

3.10 External

The External Screen allows the Admin to connect PAGIS to an external database or device via XML Datastream. This feature is Off by default and any changes must be saved before they will be available.



Enabling the Datastream:

1. Click the Off Button OFF to toggle to On ON
2. Click the Save button in the upper right corner
3. Close and reopen PAGIS

NOTE: Enabling this feature will reduce the overall performance of the PAGIS Software.

3.10.1 XML Datastream Ports

Administrators will need to configure their external device or database to utilize two specific TCP ports:

1. Query Port: TCP 7000
2. XML Datastream/Heartbeat: TCP 10100

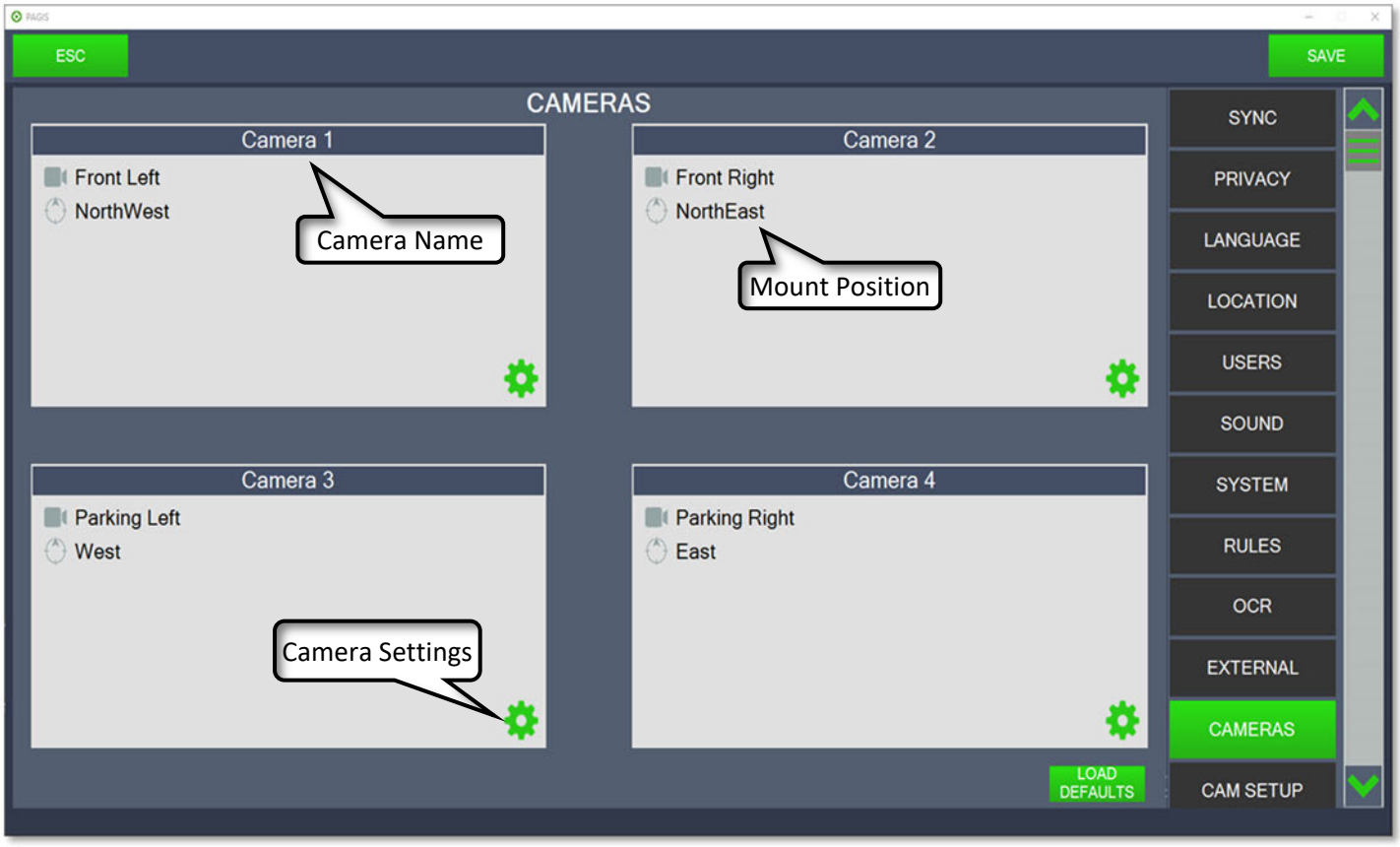
NOTE: Greater detail on the XML Datastream can be found in Appendix D

2928

3.11 Cameras

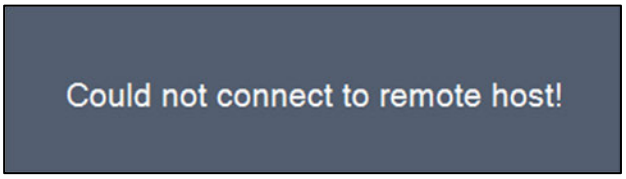
The Cameras Section provides the Administrator the means to add/delete, identify, and configure the ALPR cameras. Although the PAGIS Software comes preloaded with a default layout, best practices advise the Admin to fully review, and completely configure at least one MDC by hand in order to tailor the setup for the Agency's unique attributes.

IMPORTANT: The configuration steps completed here will dictate the available camera mode options in the Configs Section.



3.11.1 Checking the Connection

In order to configure the cameras, the PAGIS Software and the SX Processor (Black Box) must be able to communicate. If they cannot, the Administrator will receive the error message below as soon as he or she clicks on the Cameras Button CAMERAS indicating that PAGIS cannot "see" the cameras.



3.11.2 Troubleshooting Camera Connections

The most common troubleshooting steps have been included below for convenience. If these don't resovle the issue, please contact Neology Support for additional assistance. **NOTE**: For more information see Appendix C – The Mobile FAQ

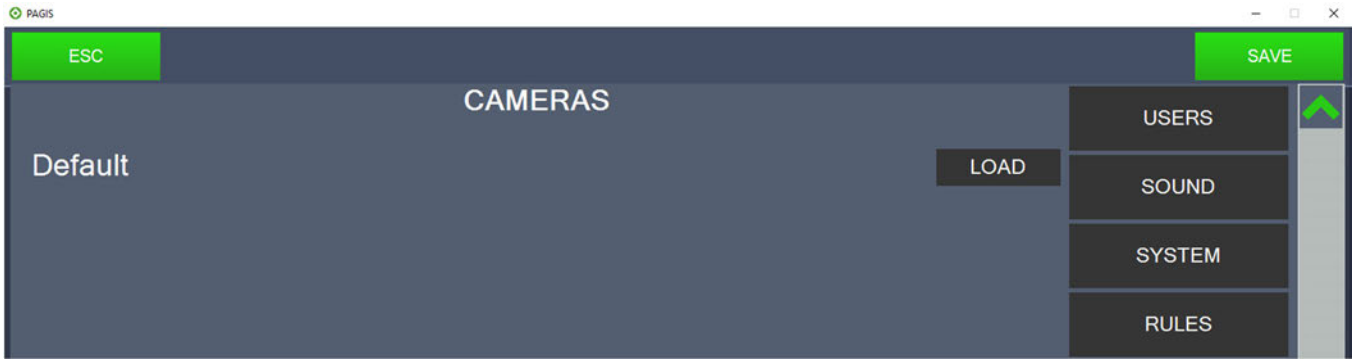
1. Start the vehicle and confirm power to the Processor. Confirm the SX switch, and any added in-line switch, is set to On.
2. Confirm the network adapter settings on the laptop match the proper Static IP scheme for the SX Processor in use.
3. Disable the local Windows Firewall, VPN software, and any real-time monitoring software one at a time.
4. Use a different network cable ensuring it's properly seating in NIC port on the SX as well as the MDC or Docking Station.
5. Docking Stations can also impede communication. Test by removing the laptop from thhe dock, directly connect the network cord to the laptop, and then reconfigure the network adapter settings as needed.

2929

3.11.3 Configuring the Cameras in PAGIS

This section will assist with the general configuration of the cameras. Administrators can begin by selecting the Settings Icon  to edit each of the existing cameras or by selecting the Load Defaults Button  . This manual will start with Load Defaults.

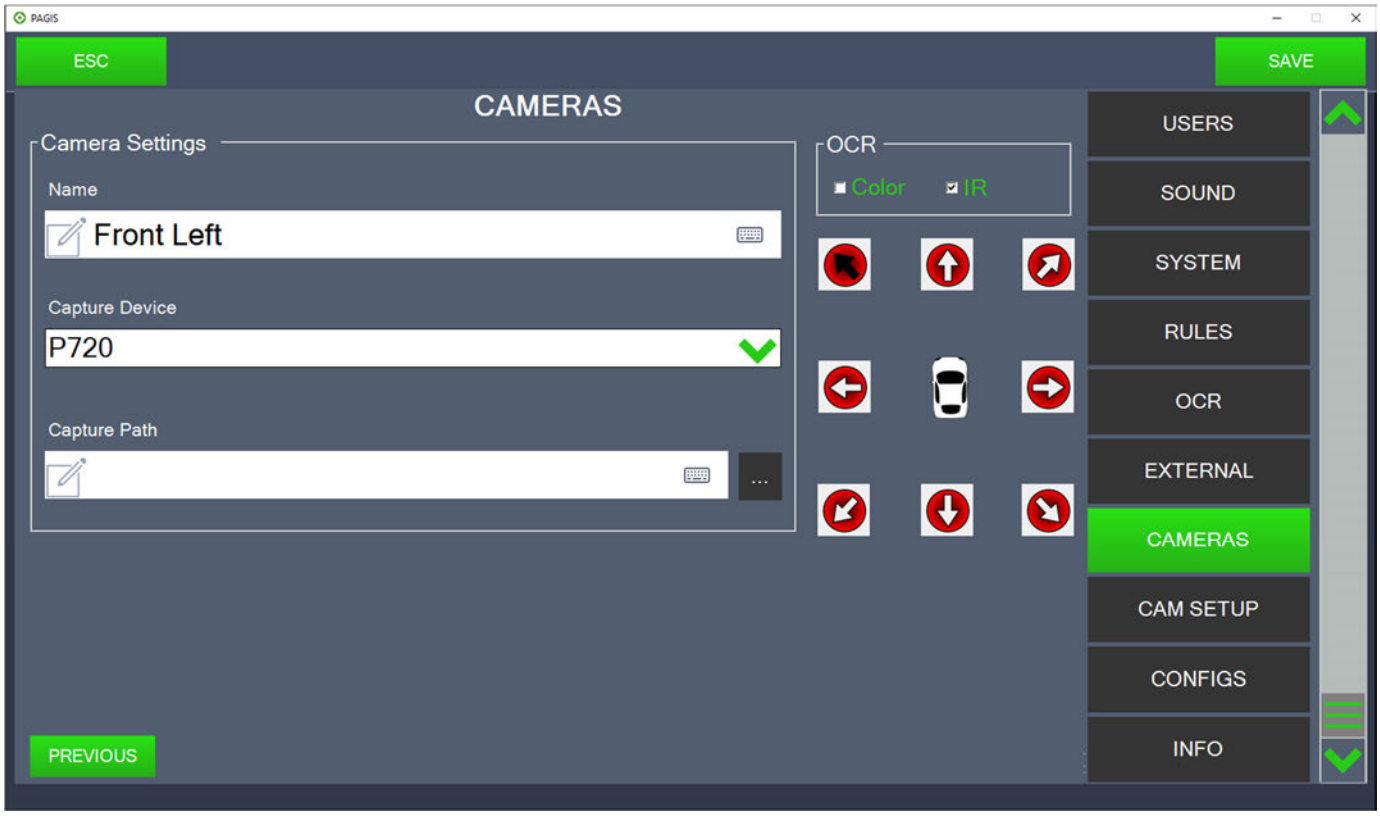
Gettings Started – Load Defaults:



1. Click the Load Defaults Button in the lower right portion of the Cameras Screen
2. Locate "Default" and click the Load Button 
3. Once it's selected (and turned Green), click the Save Button (This returns the Admin to the Cameras Screen)
4. Click the Settings Icon  to inspect and configure each camera one at a time

The Camera Settings (Edit) Screen:

This provides the Admin a single screen to edit the name, confirm the capture device, assign camera position, and confirm OCR.

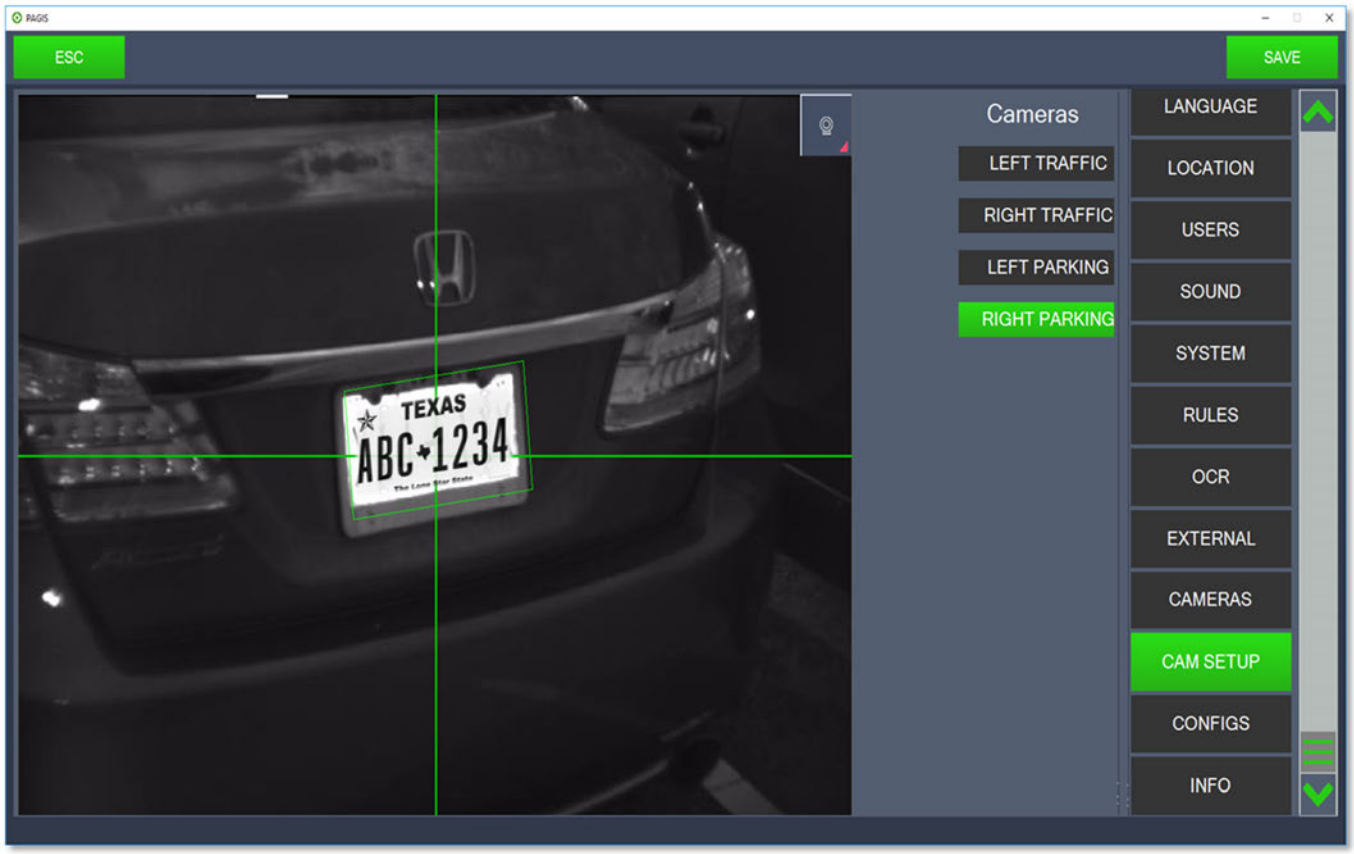


1. Confirm/Update the Camera Name **NOTE**: Use Camera Names with 11 characters or less to avoid various UI anomalies
2. Confirm the "Capture Device" field was auto-detected. If not, use the drop down to select the only Pxxx value on the list
3. Leave "Capture Path" blank (This is an optional field)
4. Select the camera mount position indicating the direction the camera is facing. The arrows turn black when selected 
5. Ensure the OCR is set to IR. The color camera is used for OCR in only rare situations and will increase system load as well as the likelihood of false alerts. Use this setting with caution
6. Click the Save Button to retain the changes

2930

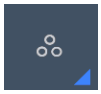
3.12 Cam Setup

The Cam Setup Screen presents Administrators with a live preview of the configured cameras. This section also allows the Admin to switch view modes from Color to IR to ensure the system is functioning properly. **NOTE**: This screen can also be utilized as a means to align newly mounted cameras when RDP access to the SX Processor is limited or unknown.



3.12.1 Cam Setup Navigation Buttons

The Admin may view the output of each camera by clicking on the camera name. When a camera is selected, the button will turn green to indicate it has been selected. In order to switch view modes, the Admin must use the following buttons:



Color View: The Color View Mode is the default view when the Admin first enters Cam Setup. This displays a live preview of the color camera.



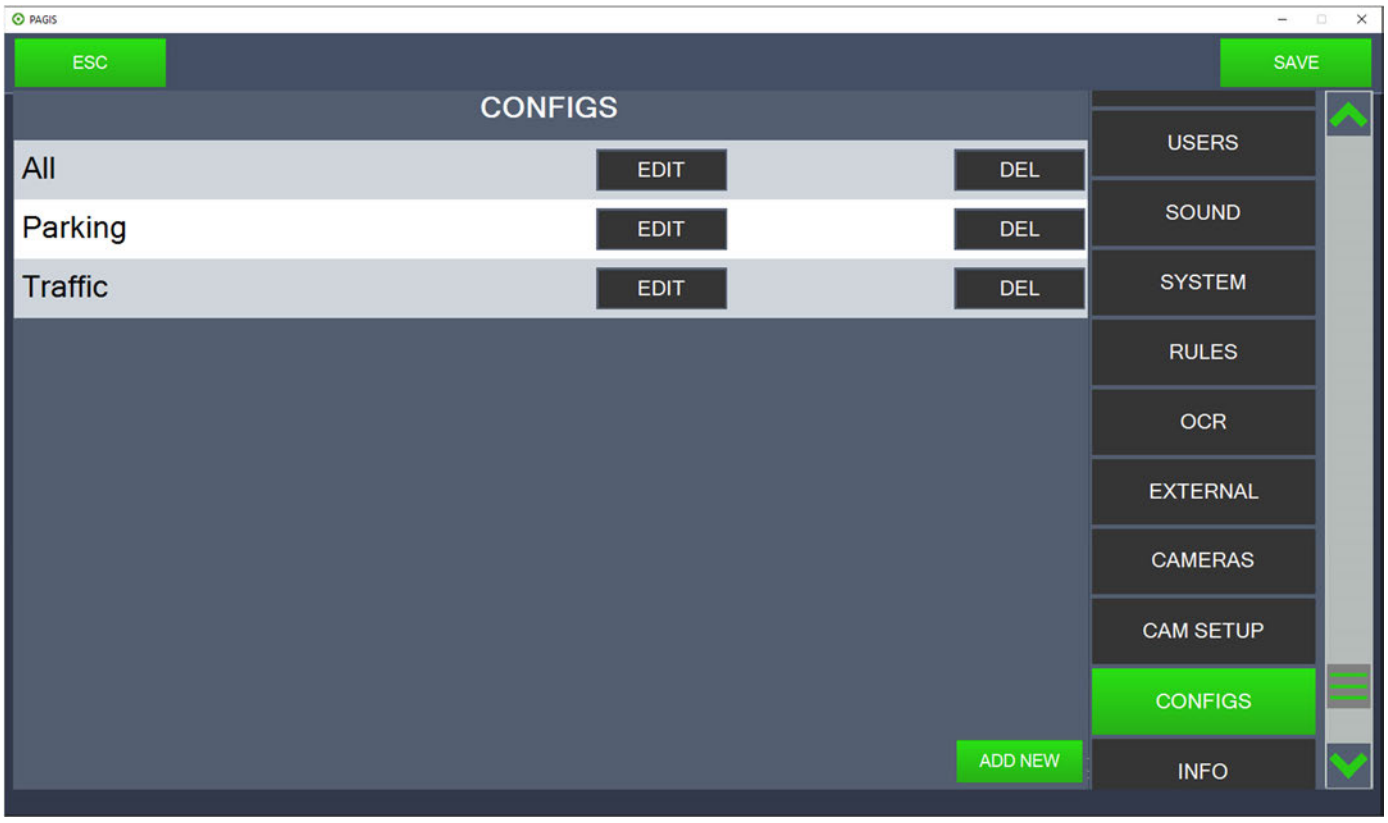
IR View: By clicking on the Camera View Selector button, the Admin will switch to the Infrared (IR) View Mode. This displays a live preview of the IR camera.

NOTE: Unlike the main Live View Screen, the camera feed shown on the Cam Setup page will not time out when in use. This feature makes it easier for the Administrator to review and align the mobile cameras.

2931

3.13 Configs (Camera View Modes)

The Configs Screen allows the Admin to construct how the cameras will be displayed on the Live View Screen for the user. This section also allows agencies to create multiple viewing configurations to meet specific environmental needs or to add greater functionality to the software. By default, the Configs layout provides the agency with three camera modes, “ALL”, “Traffic” and “Parking”. All mode dipalys the front two cameras and rear two are activated, Traffic mode only displays the front two cameras and rear cameras are off, Parking mode only displays rear two cameras and front cameras are off.



3.13.1 Configs Navigation Buttons

To properly configure the camera modes used in PAGIS, the Admin will navigate this section with the following:



To delete a config/camera mode, click the DEL button to select it (turns Green) and then click Save



To review, edit, or modify a camera mode, click the EDIT button



To preserve changes or finalize a deletion, click the SAVE button



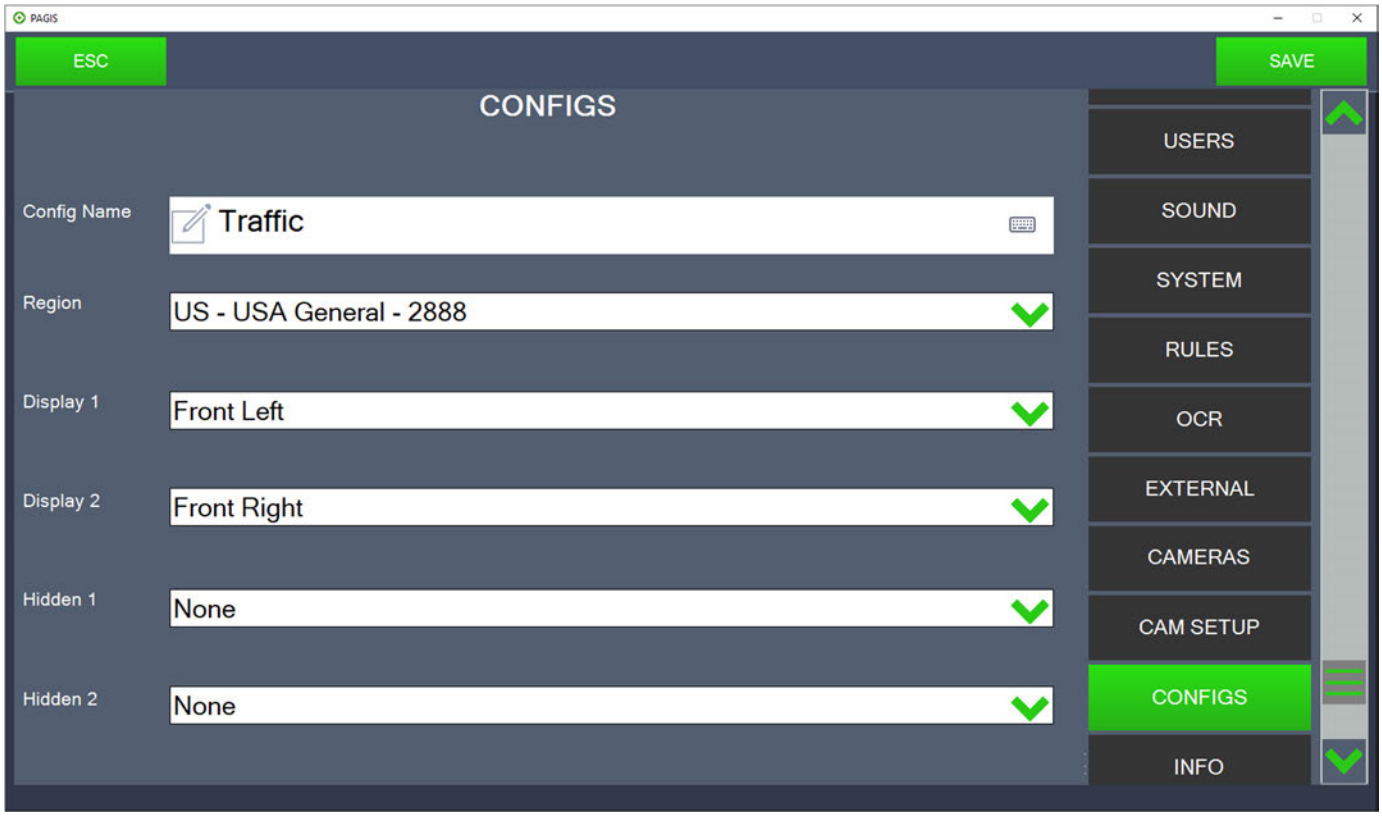
To add a new camera mode, click the ADD NEW button

NOTE: The number of Configs equals the number of Camera Modes available to the user from the Live View Screen. Each camera mode untilizes the Config name established in this section. Users cycle through the modes on the Live View Screen by clicking the Mode Selection Button in the upper left corner.

2932

3.13.2 Reviewing and Modifying Existing Modes

When getting started, most Administrators will begin by simply modifying the existing camera modes or “configs”. The following example will demonstrate the standard configuration of a four-camera mobile unit.



1. Click the EDIT Button EDIT from the main Configs Screen to modify a mode
2. Review/Update the name of the Mode **NOTE**: The name should be intuitive for all users as this becomes the label of the mode selection button on the Live View Screen
3. Click the drop down arrow on the Region field to select the best local option (Adds additional accuracy to OCR)
4. Confirm the camera listed in the Display 1 field. This camera will be displayed on the left side of the Live View Screen
5. Confirm the camera listed in the Display 2 field. This camera will be displayed on the right side of the Live View Screen
6. Confirm the Hidden 1 field shows one of the other cameras not listed in the Display fields
7. Confirm the Hidden 2 field shows the last available camera not yet listed (Leave field as “NONE” for 3-cam systems)
8. Click the Save button to retain the changes
9. Click the Configs Button from the menu to access the other Mode(s)
10. Perform steps 1-8 for all Configs/Camera Modes available

NOTE: Cameras listed in the Hidden fields will function, perform OCR, and capture plate reads, but they will not be displayed to the user while in the named camera mode (unless a Hit is detected opening the Alert Screen). For ALPR units with more than two cameras, best practices dictate the Admin utilize these fields.

3.13.3 Adding a New Camera Mode

When the two default modes provided in the PAGIS software do not offer the agency all the functionality desired, the Administrator can use the Configs Screen to add additional camera modes. For example, if officers request a mode to view only the cameras on the left side of the vehicle while stopped on the side of the road, the PAGIS Adminstrator can build that functionality from this screen.



1. Enter a name for the new Mode (Ex. “Left Side”)
2. Click the drop down arrow on the Region field to select the best local option (Adds additional accuracy to OCR)
3. Confirm the camera listed in the Display 1 field. This camera will be displayed on the left side of the Live View Screen
4. Confirm the camera listed in the Display 2 field. This camera will be displayed on the right side of the Live View Screen
5. Confirm the Hidden 1 field shows one of the other cameras not listed in the Display fields
6. Confirm the Hidden 2 field shows the last available camera not yet listed (Leave field as “NONE” for 3-cam systems)
7. Click the Save button to retain the changes

3.14 Info2934

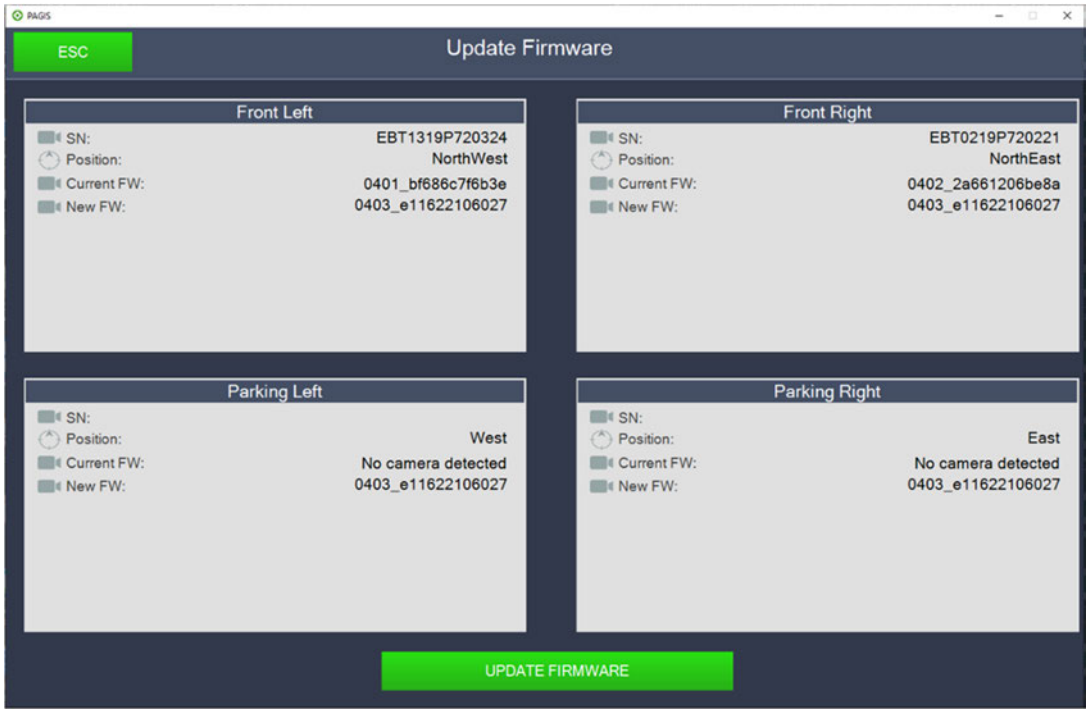
The Info screen displays additional information including the version number of the current installation. This information is helpful when contacting Technical Support.



3.15 Camera Firmware Update, (Admin)

Camera firmware update provides a means for Neology to update the camera software to enhance and or correct camera performance. The frimware icon  will only apper when a update is avialable.

- The firmware update process only updates camera that are attached and function on the mobile processor.
- Administrator must log into PAGIS and apply the FW update. The update process takes around 4min and should not be interrupted or risk permanently damaging the cameras, PAGIS will return to normal opertaion after update.
- Once the "UPDATE FIRMWARE" button is clicked PAGIS will switch to full gray screen with message indicating "Camera Firmware is Updating", during this process you'll will notice small command windows opening on top of PAGIS, these windows represent the firmware being applied to each active camera so you may notice one or server depending. Once completed a message will appear "Firmware Updated Successfully" then PAGIS will return to normal operation.
- After FW completion and return to "Live View", its requiered to cycle thought the "Cam Mods" to refresh cameras.



Firmware Updater Window List.

- Title "Camera Name".
- Camera serial number.
- Position.
- Current FW version.
- New FW version available.

4.1 PAGIS System Requirements

The PAGIS Software requires the following minimum system requirements for the mobile data computer:

- Intel I3 CPU at 2.0 GHz or higher.
- Windows Operating System (Win7-Win10).
- Microsoft .NET Framework 3.5.
- 8 GB of RAM.
- At least 1 GB of free disk space.
- SVGA display with a minimum resolution of 800 x 600 pixels.
- Available 10/100 Ethernet port.
- Keyboard and mouse, or a touch screen monitor.
- Internet access needed for mapping and Firmware update.

4.2 PAGIS Prerequisites

Prerequisites:

1. Ability to install software.
2. Ability to configure the network adapter.
3. PAGIS 2.12 and above are only compatible with SX4 and SX4e Processors.

Network Adapter Settings:

The Neology mobile processor operates based on a static IP and is preassigned the IP address of 192.168.200.201. When connecting laptop/MDC to the mobile processor your computer must be on the same IP network as the mobile processor, in fact the connecting compute must adopt one octet lower than the assigned IP of the processor in order for MDC installed PAGIS to connect to the mobile processor and receive data from the ALPR cameras. Below are the steps to configure your computer.

1. Navigate to Adapter Options in Windows and right click on the adapter and select properties.
2. Click to select IPv4 and click Properties
3. Click the radio button “Use the following IP Address” to set the Static IP address.
4. Enter 192.168.200.200 in “IP address” section.
5. Enter 255.255.255.0 in “Subnet mask” section.
6. Either leave the “Default gateway” blank or enter 192.168.200.201.
7. Click OK to save changes.

NOTE: The Mobile processor is pre-configured to relay its camera data connection to the 192.168.200.200 IP address, using alternative IP’s on MDC/Laptop will result in the software’s failure to communicate with the cameras when using VPRelay mode.

Alternative IP Network:

It is possible to configure the Neology mobile processor to utilize a different IP network in conjunction with MDC/Laptop. Typical scenario would be when mobile processor and MDC/Laptop are connected through an onboard modem that has an Ethernet switch with available ports. Below are the general steps to changing IP network.

1. Follow the step above to connected to Neology mobile processor.
2. Remote desktop to Neology mobile processor and login using credentials provided in SX4 or SX4e manual.
3. In Windows “Services” find and stop the “PIPS VPRELAY” service.
4. Navigate to “C:\PIPSTechnology\VPRelay” and located file “anpr2.ini and open in notepad.
5. Alter “Address=192.168.200.102” to the IP your MDC/Laptop will assume after change to new network, save and close. The “PIPS VPRELAY” service will use this IP address to send camera data to PAGIS running on MDC/Laptop.
6. Alter Neology mobile processors “Ethernet adapter 1” to new IP, refer to SX4 or SX4e manual for instruction on disabling the “WFManager” so change made to Ethernet are permanently saved.
7. Reboot mobile processor and enable “WFManager”.
8. Reassign IP on MDC/Laptop.
9. Start PAGIS on MDC/Laptop and confirm camera connectivity, if issues refer to FAQ’s in this manual for troubleshooting tips.

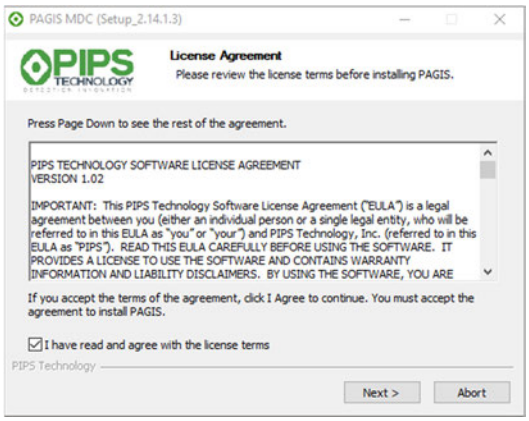
2936

4.2.2 PAGIS Software Installation (MDC)

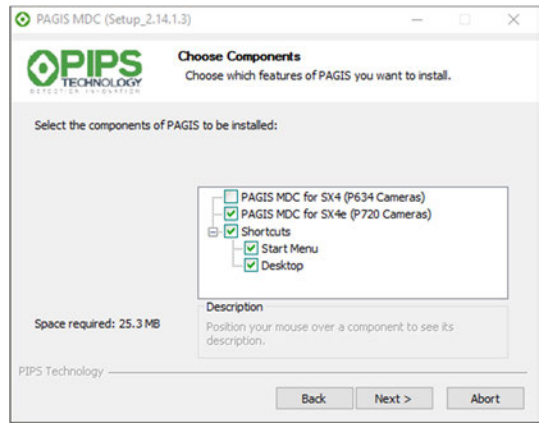
1. If PAGIS exist on your computer, it must be version 2.9 or 2.12 for installer to update. If your version of PAGIS is older it is recommended you “EndShift” any existing data, then uninstall PAGIS.
2. It is recommended you “EndShift” any existing data if upgrading a previous version of PAGIS.
3. Prior to software installation, take the time to figure out what version of Neology mobile processor you have as the software installation requires you to select options so it can properly configure the camera settings based on processor type. PAGIS version 2.14 supports processor versions SX4 & SX4e only, you can either look at the product tag located on the processor or look at the camera IO ports on the back of the processor. If the 4 camera IO ports are vertically arranged RJ45’s then it’s a **SX4e(P720)**, if they are vertically arranged circular shaped “LEMO” connectors then it’s a **SX4(P634)**. Horizonal arranged circular shaped “LEMO” connectors is a SX3 and is not compatible with PAGIS 2.14.
4. Upgrading to PAGIS V2.14.x.x also requires that the Neology mobile processor be updated to same version in order to take advantage of the Firmware updater feature.



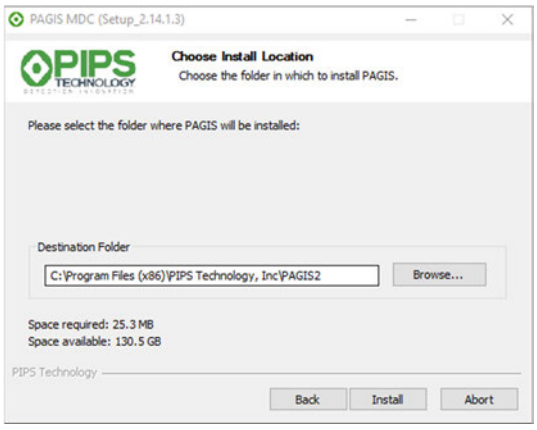
5. Place the PAGIS installer on your computer’s desktop, “PAGIS_Setup_MDC_2.14.x.x.exe”.
6. Right click the PAGIS installer executable and select “Run as administrator”.



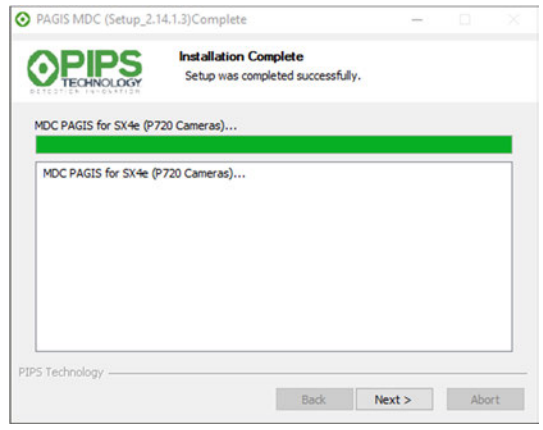
7. Check the license agreement box, then click Next.



8. Select the mobile processor type and alter “Shortcuts” if needed. Next to continue.



9. Confirm path if upgrading, click Install to proceed.



10. Installation Compete, Next to proceed.
11. Click Finish.
12. Click Yes to reboot if you would like to test PAGIS auto start at login if selected during installation, otherwise click No as its not required for PAGIS to run.

Note: See Appendix A for terminology definitions.

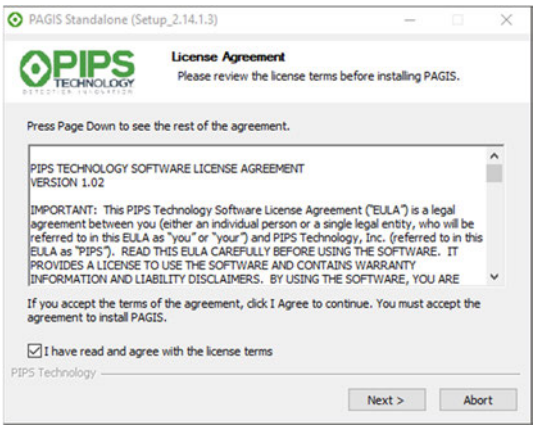
4.2.3 PAGIS Software Installation (Mobile Processor)

1. PAGIS v2.14.x.x updater is only compatible with Neology mobile processors SX4 & SX4e.
2. The PAGIS updater only updates existing versions of PAGIS on mobile processor, version 2.9 and newer.
3. Update required for both “Standalone” & “Service/VPRelay” to support some of the newer features.
4. The processor must be in its respective mode to update that option as the folder path are hidden when not active, see “Change Mode” in SX4 or SX4e manual.

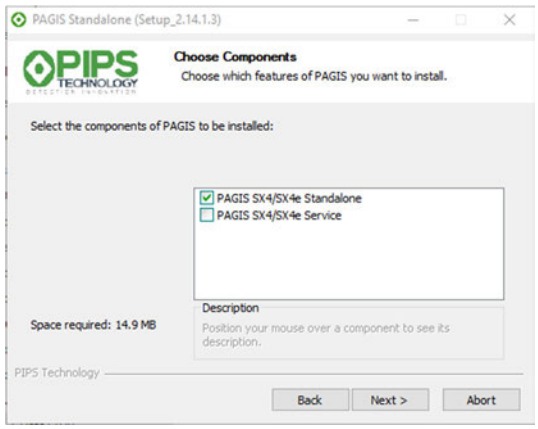
NOTE: If processor is in Service/VPRelay mode you MUST stop the “PIPS VPRELAY” service before running the updater.



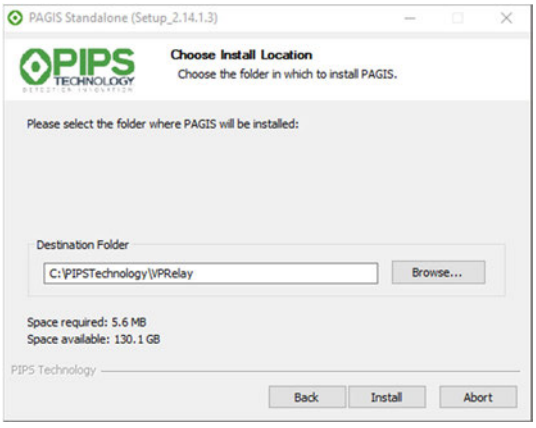
5. Remote desktop into processor or utilize attached monitor/keyboard.
6. Place the updater in C:\PIPSTechnology folder on the PIPS mobile processor.
7. Execute PAGIS Updater.



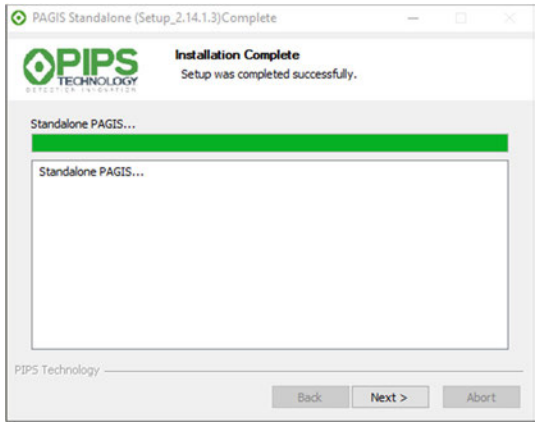
8. Check the license agreement box, then click Next.



9. Select option to update, next to continue.
   - Standalone= PAGIS login from Processor.
   - Service= PAGIS login from connected Laptop.



10. Change the default path presented by updater, see below.
    - For “Service” C:\PIPSTechnology\VPRelay.
    - For “Standalone” C:\PIPSTechnology\Standalone.



11. Installation Compete, Next to proceed.
12. Click Finish.
13. Click Yes to reboot.

Note: See Appendix A for terminology definitions.

2938

TROUBLESHOOTING TIPS

This section provides some basic troubleshooting tips and information

5.1 Troubleshooting & Tips

- The first login to PAGIS after the new install of an unconfigured version does not require a username or password. Simply click Login to be granted Admin access to the software.
- A good means to test the communication from the MDC to BOSS is ping or telnet (over TCP 8092) through the command prompt.
- A good means to test the communication from the MDC to the SX Processor is ping or telnet (over TCP 9000) via command prompt.
- For many other troubleshooting tips, see Appendix C – Frequently Asked Questions

5.1.1 PAGIS with NetMotion VPN

Agencies utilizing NetMotion VPN software on the MDC will need to apply the following passthrough steps:

1. Login to the NetMotion server as administrator
2. Click Settings > Then select Client > Select Global Client Settings > Then select Passthrough List
3. Click the “Add…” button on the right > Select “Network Address”
4. Enter the following settings (as shown):
    A. IP address:192.168.200.0 (the zero is correct, it's an IP address “range”) Subnet Mask: 255.255.255.0.
    B. Keep all other settings default (as shown) and click OK.
5. The MDC must then disconnect from NetMotion and reconnect again for the settings to be applied locally.

5.1.2 Cisco VPN Client:

Make sure Stateful Firewall is unchecked and "Allow Local LAN".

5.1.3 Microsoft .NET 3.5 Installation

The PAGIS Software requires Microsoft .NET Framework 3.5 specifically. If the MDC doesn’t have .NET, it can be downloaded from the Microsoft website.

5.1.4 Firewall Settings for Client-Server Installations

For client-server installations, the Windows Firewall needs to allow the SX Processor and the MDC to communicate. If the MDC is maintained by a Network Administrator, he or she should be contacted before making changes to the firewall. The command prompt commands for the exceptions are below

Option 1: Allow Microsoft Windows Version 8 or newer to auto-detect the launch of the PAGIS.exe application and use the wizard to add the PAGIS.EXE to the exception list (making note of Public or Private Network settings as necessary).

Option 2: Add PAGIS to the exception list manually by browsing to the install path of PAGIS. The default is below for reference: C:\Program Files (x86)\PIPS Technology, Inc\PAGIS2\PAGIS.exe

Option 3: Add the communication ports manually:
TCP in/out 8092 = Pagis sync port to BOSS back office software.
TCP in/out 9000 = Mobile processor camera feed port.
TCP in/out 9001 = Mobile processor camera snapshot port.
TCP in/out 32023 = Mobile processor camera setup port.
TCP in/out 10000 = Mobile processor data capture port.
NOTE: XML Datastream uses TCP 10100 and TCP 7000

2939

PAGIS/BOSS3 CONFIGURATION

In order for the PAGIS software to function properly, the device must be built, enabled, and configured in BOSS3 before being deployed for service in the field.

6.1 Creating a New Device in BOSS3

Once network communication to BOSS3 has been established from the vehicle, the new device must be "built" or added to the Device List in BOSS3 before it can be used. The approved way to do this, is to simply perform a Begin Shift from the PAGIS software. **NOTE**: The computer name is what will be displayed in BOSS as device name.

1. At the PAGIS Live View Screen, click the Begin Shift button once to select it, and then click again to launch the sync.
2. If the laptop has previously been setup to communicate with BOSS and is already enabled, the sync transfer window should appear in the middle of the Live View Screen.
3. If this is a new/disabled device, a message indicating "HttpStatusCode" will be displayed.
4. This indicates the BOSS3 server has received the sync request but has rejected it due to device status.
5. Once the BOSS Admin has enabled the device, the Status Code error will not appear again, and syncs should complete as configured in BOSS3.

6.2 Enabling a New Mobile System in BOSS3

Installing PAGIS and configuring the network settings is only the first step in making the ALPR unit operational. Once PAGIS is configured to work with or on the SX Processor and the mobile cameras, it must then be enabled in BOSS3 before synchronizations can take place. **NOTE**: By default, every new device recognized by the BOSS3 server is disabled until the Admin enables it. This is done for security.

1. Log into the BOSS3 UI Client Software with Admin privileges.
2. Click the Admin button on the left to expand the options.
3. Click the Devices button. The new device should now be listed to the right.
4. Click the name of the Device to select it. (This will open the device details screen)
5. Click the Edit button at the bottom of the window.
6. Click the Enable button from the Edit window.
7. This will enable the device and return the Admin to the Device List.

NOTE: If desired, the Admin can re-enter the Edit window to assign an alternate name in BOSS3 for the new device. The Admin will need to update the "Description" field and then click the Save button. Agencies commonly use this field to signify the Unit number, Car name, or Patrol Shift. The "Name" field is the device/host name and cannot be edited in BOSS3.

NOTE: Once the Device is enabled the Admin needs to assign ownership and hotlist distribution.

6.3 Assigning Ownership to a Device in BOSS3

Every new device added to BOSS3 allows for Admin level access into PAGIS without the use of a username or password. In order to password protect the PAGIS software, the BOSS Administrator must assign "Owners" to the device in BOSS3.
NOTE: For more detail on Users, User Groups, Sites, and Roles, refer to the BOSS3 manual.

1. Login to the BOSS3 UI with Admin credentials.
2. Click the Admin button on the Left to expand the options.
3. Click Devices to review the list.
4. Click on the Device Name to open the device details screen.
5. Click on the Edit button.
6. Locate the "Owners" field. Click the Select button to the right.
7. Check the box(es) for the appropriate Site(s)/User Group(s). **NOTE**: This tells BOSS3 which sets of users will have rights to login to PAGIS from this specific device.
8. Notice the Select button has changed to a Save button. Click Save to retain changes.
9. Confirm the changes show in the Owners Field.
10. Click the Save button at the top left of the Edit window.

2940

6.4 Assigning Hotlists to a Device in BOSS3

In order for the PAGIS users to receive alerts, one or more of the stored hotlists in BOSS3 must be distributed to the new device. **NOTE**: For more information on building and configuring Hotlists, refer to the BOSS3 manual.

1. Login to the BOSS3 UI with Admin credentials.
2. Click the Admin button on the Left to expand the options.
3. Click the “Hotlists” button to review the list of configured alert lists.
4. Click the Hotlist Name to select the first alert list. This will open the Details screen.
5. Click the Edit button at the bottom of the window.
6. Locate the “Deployment” field. Then click the Select button to the right.
7. Check the box next to the name of the new device.
8. Notice the Select button has changed to a Save button. Click Save to retain the changes.
9. Confirm the changes show in the Deployment Field.
10. Click the Save button at the top left of the Edit window.
11. Perform these steps again for all remaining Hotlists necessary for this device.

PAGIS/BOSS4 CONFIGURATION

In order for the PAGIS software to function properly, the device must be built, enabled, and configured in BOSS4 before being deployed for service in the field.

7.1 Creating a New Device in BOSS4

Once network communication to BOSS4 has been established from the vehicle, the new device must be “built” or added to the Device List in BOSS4 before it can be used. The approved way to do this, is to simply perform a Begin Shift from the PAGIS software. **NOTE**: The computer name is what will be displayed in BOSS as device name.

1. At the PAGIS Live View Screen, click the Begin Shift button once to select it, and then click again to launch the sync.
2. If the computer has previously been setup to communicate with BOSS and is already enabled, the sync transfer window should appear in the middle of the Live View Screen.
3. If this is a new/disabled device, a message indicating “HttpStatusCode” will be displayed.
4. This indicates the BOSS4 server has received the sync request but has rejected it due to device status.
5. Once the BOSS Admin has enabled the device, the Status Code error will not appear again, and syncs should complete as configured in BOSS4.

7.2 Enabling a New Mobile System in BOSS4

Installing PAGIS and configuring the network settings is only the first step in making the ALPR unit operational. Once PAGIS is configured to work with or on the SX Processor and the mobile cameras, it must then be enabled in BOSS4 before synchronizations can take place. **NOTE**: By default, every new device recognized by the BOSS4 server is disabled until the Admin enables it. This is done for security.

1. Log into the BOSS4 URL with Admin privileges.
2. Navigate to the Resources pulldown menu.
3. Select Devices from the menu options. The new device should now be listed.
4. Click the name of the Device to select it. (This will open the device details windows on the left)
5. Click the Enable slide toggle to enable device, located in upper right of device edit window then click save.
6. This will enable the device, synchronization between BOSS4 and PAGIS is allowed.

NOTE: Once the Device is enabled the Admin needs to assign ownership and hotlist distribution.

2941

7.3 Assigning Ownership to a Device in BOSS4

Every new device added to BOSS4 allows for Admin level access into PAGIS without the use of a username or password. In order to password protect the PAGIS software, the BOSS Administrator must assign “Owners” to the device in BOSS4.

NOTE: For more detail on Users, User Groups, Sites, and Roles, refer to the BOSS4 manual.

1. Login to the BOSS4 URL with Admin credentials.
2. Navigate to the Resources pulldown menu.
3. Select Devices from the menu options. The new device should now be listed.
4. Click the name of the Device to select it. (This will open the device details windows on the left)
5. Locate the “Owner” field. Click in the Owner filed, and a list of all available Groups will appear.
6. Select group by clicking on it, it will then automatically be added to owners, see list below “Owner”.
7. To add mode groups, repeat step 15.
8. Confirm the changes show in the Owner Field.
9. Click the Save button at the bottom right of the Edit window.

7.4 Assigning Hotlists to a Device in BOSS4

In order for the PAGIS users to receive alerts, one or more of the stored hotlists in BOSS4 must be distributed to the new device.

NOTE: For more information on building and configuring Hotlists, refer to the BOSS4 manual.

1. Login to the BOSS4 URL with Admin credentials.
2. Navigate to the System pulldown menu.
3. Select Hotlists from the menu options
4. Click the Hotlist Name to select the first alert list. This will open the Details screen.
5. Locate the “Deployment” field.
6. Check the box next to the name of the new device listed.
7. Click the Save button at the bottom right of the Edit window.
8. Perform these steps again for all remaining Hotlists necessary for this device.

APPENDIX A: THE GLOSSARY

ALPR/ANPR	"Automatic License Plate Recognition/Automatic Number Plate Recognition".
BOSS	"Back Office System Software". This is the ALPR server.
GPS	"Global Positioning System".
GUI	"Graphical User Interface".
Hotlist	A database or list that contains vehicle license plates of interest ("alert list").
IR	Infrared light.
License Plate	Also called a tag or number plate.
MDC	"Mobile Data Computer". This is the tablet or laptop in the vehicle.
OCR	"Optical Character Recognition" (also referred to as a "cardet").
OS	"Operating System".
PAGIS	This is the License Plate Capture Software most commonly used in an ALPR vehicle.
Service	Operation mode of the PAGIS software. Service or "VPRelay" is used to refer to PAGIS instance that is running directly on the Neology mobile processor without a GUI interface, this mode is intended to run in conjunction with MDC version of PAGIS installed on laptop connected via Ethernet.
Standalone	Operation mode of the PAGIS software. Standalone is used to refer to PAGIS instance that is running directly on the Neology mobile processor with a GUI interface. Same a "Service"
SX	SX is a short notation referencing Neology mobile processor, commonly the SX is followed by the generation number of the processor, i.e. SX3, SX4 & SX4e.
UI	A "User Interface" is the means in which the user can access and navigate the software.
USB Flash Drive	Also called a thumb drive or memory stick.
VLP	"Vehicle License Plate".
VPN	"Virtually Protected Network".
VPRelay	Operation mode of the PAGIS software. VPRelay or "Service" is used to refer to PAGIS instance that is running directly on the Neology mobile processor without a GUI interface, this mode is intended to run in conjunction with MDC versions of PAGIS installed on laptop connected via Ethernet.
Whitelist	Opposite of a standard BOSS Hotlist. This is a list of license plates that should not trigger an alert.

2943

APPENDIX B: PAGIS SOFTWARE DATABASE FILE

This section is used to configure the PAGIS Software when it's not being used with the Back Office System Software (BOSS). Comma-separated value (CSV) format is the only format the PAGIS Software supports for importing data into the vehicles for the purpose of matching against the captured license plate data. PAGIS will support CSV files with any number of columns, called "fields", as long as the first field is the VLP (Vehicle License Plate). **NOTE**: The CSV format is standard ASCII.

Example CSV Files:

1. *ABC123, Red, Ford, Explorer, 1996, WANTED XYZ456, Blue, Audi, A4, 2001, MURDER*
2. *45ABC234, Vehicle wanted in associated with a kidnapping on 12/5/2005 995BD233, Vehicle reported stolen from Liz's Lounge at 6am on 12/1/2005*
3. *UIO223 ABC123*

General Function:

PAGIS calls/utilizes files in pairs. Each database in PAGIS is created using two files; a CSV file, and an INI configuration file. Without both of these files, the database will not load and PAGIS will not "see" it. Each CSV file/hotlist must have the exact same name as the INI configuration file. Example: Stolen.ini and Stolen.csv will work. Stolen.ini and Plates.csv will not.

Reading an INI Configuration File

Lines that appear in brackets [] are called "Headings". The labels that appear inside the headings, are called "values". Values will always contain an equal sign (=). If a line starts with a semicolon, it is considered to be a comment and is not read by the software. There is no limit to the number of comments in the INI file.

The [SETTINGS] Heading

The values in the Settings heading are: NumFiles, DbName, DbColor, Priority, Covert, Alarm, and NumFields.

- NumFiles: Determines how many database files the system should split the specified hotlist into. Generally, this value is set to 1. But for larger hotlists (200,000+ lines), a number of 2-5 may be more desirable.
- DbName: Tells the PAGIS Software what the displayed name of the hotlist should be.
- DbColor: Sets the display color of the hotlist. This is merely an esthetic setting and not a functional setting. The right-hand side of the equal sign is the HEX value representing the ARGB values for the color. If this value is unknown, the Admin should simply leave this line out of the file.
- Priority: Designates the priority of this hotlist in relation to other hotlists in the system. The highest priority database is 1 and the lowest is 999. **NOTE**: if a plate resides on multiple lists the higher priority will be alerted first.
- Covert: Determines whether standard PAGIS Software users are alerted when a hit is made from the database. Covert database can be used for hotlists that are included for information-gathering purposes rather than eliciting user intervention. The system can also be configured to notify via email or SMS message when a hit is made from a covert hotlist.
- Alarm: Sets the audible alert to be played in PAGIS when a hit is made from the hotlist. Values for Alarm are LOW, MED, HIGH
- NumFields: Indicates how many fields (columns) are in the CSV file. If this value is less than the actual number of fields in a file, then the additional fields are placed in the general information area. This value also determines the number of headings of the [Field x] present in the file. For example, if NumFields=2 then there will be two additional headings, [Field 0] and [Field 1]. **NOTE**: Adding "Creation =" will place the timestamp the hotlist was added to the Begin Shift file.

2944

The [FIELD X] Heading

Under the Field heading, there are two configurable values, “Name” and “PAGIS”.

- Name: Tells the system what the name of this field is. If no name is specified, then no name given to the field. The format is Name = <field>
- PAGIS: Specifies how to display the field in the GUI/PAGIS Software.
  - If no value is defined, the field is placed as general information.
  - Values 1-5 represent special fields for the PAGIS Software that translate to the information being displayed in a box of its own when a hit is processed.
  - A value of 6 represents an ID number to cross reference the vehicle from the hotlist with a person from the wanted list.
  - A value of 7 is identical to leaving the value undefined.

Sample INI Configuration File

[Settings] NumFiles=1
DbName=Stolen Vehicles DbColor=ffffff00 Priority=5 Covert=False Alarm=MED NumFields=8
;PAGIS Values
;0 is VRM / VLP (Not User Definable, always Field 0)
;1 is Special Field 1
;2 is Special Field 2
;3 is Special Field 3
;4 is Special Field 4
;5 is Special Field 5
;6 is ID Number (PNC ID, Driver’s License, Social Security Number, etc.)
;7 is General Info (Default for all undefined fields) [Field 0]
PAGIS=VRM

Sample INI Configuration File

[Field 0] Name=VRM
[Field 1] Name=Color
PAGIS=3 [Field 2]
Name=Make PAGIS=1
[Field 3] Name=Model
PAGIS=2 [Field 4]
Name=Action PAGIS=4
[Field 5] Name=Warning
PAGIS=5 [Field 6]
Name=PNCID PAGIS=6
[Field 7] Name=Intelligence PAGIS=7

To deploy a locally created hotlist to PAGIS without BOSS.

1. Create a folder called “beginshift” (Without Quotes) on the root drive of whatever drive media your using that PAGIS has access to, remember only on root drive, no subdirectory’s. Example C:\beginshift.
2. Place the .CSV & .INI in the newly created beginshift folder.
3. Log into PAGIS and configure Sync to access the drive where your file/files are located. When setting disk drive letter in PAGIS no need to indicate folder path as PAGIS assumes by default that “beginshift” exist on the root drive your selecting, refer to section 3.1 in this manual.
4. Go back to main screen and do beginshift.

2945

APPENDIX C: FAQ

Q: **HOW DO I ENTER A SUPPORT CASE?**
A: We have a webform you can use here, you can email our Support Team at Alpr_support@neology.net, or you can call us on the phone Monday-Friday 8am to 4pm Central Time (9am-5pm Eastern) at (833) 747-7577 Option 2.

Q: **HOW DO WE CREATE USERS IN PAGIS?**
A: The agency BOSS Administrator creates all users, both for BOSS and for PAGIS. Once the user is created in BOSS, the Admin would click the user's name to select/edit the user. Then click the Advanced button and update the PAGIS specific password. Please note that the username and password fields are both case sensitive and the PAGIS users need to be added to a group with the Role that allows them to use PAGIS/LPCS.

If you have any further questions, please feel free to enter a request for support here.

Q: **WHERE DO USERS CHANGE THEIR LOGIN PASSWORD IN PAGIS?**
A: User passwords are created and updated in BOSS via the UI client software. For the majority of our customers using both the PAGIS Software and BOSS, any user accounts or passwords created in the PAGIS Software itself will be overwritten by the user information defined in BOSS during the next sync.

If you have any further questions, please feel free to enter a request for support here.

Q: **HOW DO WE REQUEST AN RMA REPAIR?**
A: To assist with this, please navigate here to review our RMA procedure as well as to download the request form. Please keep in mind that once submitted, all repairs are reviewed for age of equipment and warranty status before final processing takes place. Additionally, incomplete forms and those without much detail often result in processing delays.

If you have any further questions, please feel free to enter a request for support here.

Q: **WE GOT NEW MDC LAPTOPS IN THE PATROL CARS, HOW DO WE ADD THOSE DEVICES TO BOSS?**
Q: **HOW DO WE EDIT THE DEVICE NAMES IN BOSS?**
A: The initial device template/skeleton is automatically created in BOSS the first time the device attempts to Sync from the field. Devices should NEVER be created manually. For PAGIS laptops, this is done after PAGIS is installed and configured and Begin Shift is launched. However, if the agency would like to organize the device list by updating the "Device Name" field, those steps are below:
1. Login to the BOSS UI with Admin rights
2. Navigate to Admin > Devices
3. Click on a device name to select it > Click Edit
4. Update the name of the device in the "Description" field (Name field cannot be altered)
5. Click Save > This will take you back to the Device Summary List. The "Device Name" field should show the new name

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WE HAVE A NEW MOBILE COMPUTER/MDC THAT'S NOT SYNCING WITH BOSS.**
Q: **WE KEEP SEEING AN HTTP_STATUS_CODE ERROR WHEN RUNNING BEGIN SHIFT.**
A: This error most commonly means that a new device in the field (laptop/tablet) can "see" the BOSS server, but that it hasn't been enabled yet to "talk" with it. Follow the general steps below to address this issue:
1. The agency BOSS Administrator will need to login to the BOSS UI client and Select Admin
2. Then select Devices and from there, left click on the device/computer name of that MDC to edit it
3. Once in the Edit screen, Enable the device. This will take you back to the Device List.
4. Click the name to edit the device again. Now assign users/Owners and save.
NOTE: The Select button becomes a Save button when selecting which Groups/Users should have access to login to this device

5. Once that is done, navigate to Admin > Hotlists
6. From here, click on each hotlist one at a time to distribute them to the new device being sure to Save the changes next to the Distribution field. Note again that the Select button becomes a Save button. And there's another Save button at the top left of the edit window.
7. After this is complete, perform Begin Shift from the field unit/MDC and confirm there are no further errors.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **NEW PAGIS USER CAN'T LOGIN BUT OTHERS CAN.**
Q: **USERS CAN LOGIN TO PAGIS WITH NO CREDENTIALS AT ALL.**
A: Entry or login to the PAGIS software in the field is partially controlled by the Device settings in BOSS. The users themselves must also be properly setup with an LPCS/PAGIS password. To check the current device settings/ access, perform the following steps:
1. Login to BOSS UI (with Administrator rights)
2. Select the Admin Section
3. Select Devices and then Select the Device in question by PC name
4. Once selected click on the Edit button near the bottom
5. Locate and inspect the "Owners" Field (this is a list of users/groups that have access to login to the device)
NOTE: If this field is blank, the device is in an open configuration mode allowing admin level access simply by clicking login (any credentials would also be accepted).
6. To update the device owners, click the "Select" button next to the Owners field (notice it changes to a Save button)
7. Check which Users/Groups of Users should be able to login to PAGIS from this device
8. Click the Save button next to the field
9. And then click Save in the upper left portion of the Edit window
10. Have a previous user or Admin login to PAGIS and perform Begin Shift to sync the new data
11. A PAGIS Admin can confirm by navigating to Admin, Admin, and then Users to review the list
12. Another test would be to have the new user attempt to login

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WHEN USERS LOGIN TO PAGIS, THEY ONLY SEE A GREY SCREEN.**
Q: **CAMERAS AREN'T SHOWING UP IN PAGIS ANYMORE.**
SEE ALSO: "THE LINK LIGHTS ON OUR ALPR COMPUTER/MDC WON'T TURN ON OR FLASH"
A: Below are some basic troubleshooting steps you'll want to follow before creating a support ticket.
1. Doublecheck the physical power switch on the black box/Processor is On. In many vehicles, there is also an in-line switch in the front of the vehicle that needs to be switched On. When the units are properly powered and on, you should see lights and hear fans running.
2. Confirm that the network adapter settings on the laptop match the proper Static IP scheme for the SX Processor in use. The older scheme is 192.200… and the newer scheme is 192.168…. NOTE: the adapter status in Windows should say "unidentified network". If it says "cable unplugged" the laptop can't "see" the SX.
3. If the power and Static IP settings are good and things still aren't working, test further by disabling the three main software related culprits. Turn off/bypass the local Windows firewall, antivirus, and VPN software one at a time.
4. If you're still not able to see the camera feed after that, you may want to use a different network cable as those can get damaged over time and then confirm that the cord is properly plugged into the ports.
5. If the network cord from the SX Processor is routed through a docking station, then it's possible the dock is preventing the traffic. You should contact the dock's manufacturer for the most recent firmware. To test for this, remove the laptop from the dock, directly connect the network cord to the laptop, and then reconfigure the network adapter settings (remove the static settings from the dock's adapter/ and assign the static IP to the laptop's NIC adapter).

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.
Q: **THE LEFT FRONT CAMERA ON OUR ALPR VEHICLE IS NO LONGER SHOWING IN PAGIS**?
Q: **HOW DO WE TROUBLESHOOT MOBILE CAMERAS**?
A: Below are the main troubleshooting steps to test the camera(s) and cable(s) on a system where only one or two cameras are

no longer displaying images.
Step 1: Confirm MDC/SX communication - steps shown in section “Cameras aren’t showing up in PAGIS anymore.”
Step 2: Access the SX Processor – RDP or directly connect a monitor, keyboard, and mouse to the SX. Contact Neology Support for help with RDP if the credentials are unknown to the agency.
Step 3: Confirm camera activity – Launch Tools. Then open P6Utility or Mobile Toolkit. Check the camera feeds/function by switching the Input menu to the camera(s) in question
Step 4: Unplug and Reattach the Camera Cables – Note, the cables DO NOT TWIST. The metal locking nut on the cable slides back about a millimeter and the cable comes straight out. Do this at the SX Processor and the Camera. You may need to remove the camera from the mount in order to unplug the cable successfully (most brackets use a #3.5 Hex/Allen Wrench)
Step 5: Swap Port on SX Processor – At the SX Processor, swap the camera cables from the non-working camera to a port with a working port (Take care to note the swap so the cables get back to their original ports). If the camera outage stays at the port site, the issue is most likely the capture card on the SX Processor and will require RMA (Example: working Left cam is swapped to port of non-working Right cam and no longer functions. AND the previous non-working Right cam starts working once it’s plugged into the Left cam’s port). If the fault/error stays with the camera regardless of SX port, continue to Step 6.
Step 6: Physically Swap Camera Locations – Once all other items are checked, move the camera itself to a working position in order to test the cable. (Example: physically move Left cam to the Right cam position on the top of the vehicle) Connect the cable at the new position and test feed in Tools > P6Utility/Mobile Toolkit. If the camera works at the new location, the issue is most likely a bad cable. If the camera still does not work, the issue is most likely a faulty camera in need of repair/RMA.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WE’RE NO LONGER GETTING GPS IN PAGIS.**
Q: **WE’RE NOT SEEING GPS DATA FROM SOME OF OUR FIELD UNITS IN BOSS.**
A: Below are the basic troubleshooting steps for checking the GPS of field units:
1. Login to PAGIS (as Admin)
2. Navigate to Admin section, then click the Admin button
3. Select “System” on the left pane
4. Confirm/Set the button at top to “Default”
5. Remove any value(s) stored in the GPS Connection String field. Leave ‘5’ in the Computer String.
6. Click the Save button to retain changes made.
7. Close PAGIS fully and relaunch and log back in to test (Note: GPS will only show with test reads/hits)
8. For versions of PAGIS 2.9 and up, test with a GPS Connection String of 6 if the blank field doesn’t work. Save the changes. Log out. Close the software and then relaunch to test.

Please be advised, that some GPS issues can be caused by local or domain firewall settings, antivirus software, or any other software package monitoring/transmitting network data. To test these, disable or bypass those software options on the MDC and retest.

If these initial troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **HOW DO I INSTALL THE PAGIS SOFTWARE?**
Q: **I JUST LOADED PAGIS ON A MACHINE AND IT CRASHES WITH A .DLL ERROR WHEN I TRY TO LAUNCH IT.**
A: The most common installation of PAGIS is Client/Server or “VPRelay Mode”. The .dll error is caused by the installer not being run from the HDD and/or the wrong install option being selected (Example: SupeRex instead of MDC). The best practices for the installation are below. (Note, this does not cover MDC or PAGIS configuration, only the act of installation)
1. Always copy the installer over to the HDD/Desktop of the MDC. Never run it from a thumb-drive or network share
2. Regardless of how you're logged in to Windows, right click the installer and select "run as Admin" or "run with elevated privileges"
3. Continue through the message/error about OS compatibility
4. Click next on the wizard and then be sure to select the MDC option (to use with VPRelay)
5. After that, it's next, next, next, finish the reboot is not necessary

If these steps did not resolve the issue, please feel free to enter a request for support here.

Q: **USERS ARE GETTING HITS/ALERTS ON PREVIOUSLY RECOVERED STOLEN PLATES.**
Q: **USERS AREN'T GETTING HITS FROM KNOWN ACTIVE PLATES.**
Q: **THE HOTLISTS IN PAGIS DON'T SHOW TODAY'S DATE.**
Q: **THE HOTLISTS AREN'T SYNCING WITH BEGIN/END SHIFT.**
A: Whether it's from data latency or just use over time, the local file structure can get some minor corruption and will need to be refreshed. The steps below show the best practices:
1. Login to Windows with Admin rights (ability to uninstall/delete software)
2. Login to PAGIS and perform an End Shift
3. When complete without error, Logout of PAGIS and then Exit/Close the program
NOTE: If the End Shift fails or displays an error, contact Support for additional assistance.
4. If there were no errors, locate the PAGIS icon on the desktop.
5. Right click on the icon and select "Open File Location" (This should open a window where the program was installed)
6. Scroll up and locate the folder labeled "data". Double-click it to open it
7. Select and delete everything in here EXCEPT for "Attributes.db"
8. Once that's complete, Login to the PAGIS software again
9. Perform a Begin Shift. This will pull down fresh data from the server
NOTE: Once complete, the files in the data subfolder as well as the Databases section of PAGIS should be restored.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **IS PAGIS COMPATIBLE WITH OUR NEW WINDOWS 10 LAPTOPS?**
A: Although there's a warning about compatibility during the install of PAGIS on any Windows OS after XP, it is compatible with all them. However, we have seen errors occur when agencies copy and paste folder structures from previous installations. This of course is not recommended.

Q: **THE LINK LIGHTS ON OUR ALPR COMPUTER/MDC WON'T TURN ON OR FLASH.**
Q: **OUR WINDOWS 10 MDC WAS WORKING BUT HAS STOPPED COMMUNICATING TO THE SX PROCESSOR.**
A: There are many variables with troubleshooting any network connection. And the connection from the ALPR computer to the SX Processor is no different. The following troubleshooting list highlights the most common:
1. The physical network cord is bad/damaged.
A: Test with a different cable and confirm that it is plugged in fully

2. The network adapters are not configured or have incorrect static IPs
A: Confirm the Static IP scheme in use and properly configure the network adapters

3. Local and/or Domain Firewall rules have prevented the flow of communication
A: Disable or bypass these and test again

4. VPN, Anti-Spyware, Antivirus, or other monitoring software has blocked communication
A: Disable or bypass these one at a time and test after each to find the culprit(s)

5. Docking Station Firmware can be incompatible with some newer computers or become corrupt
A: Test by running the network cord straight to the MDC and then configuring the network adapters (NOTE: It would also be a good idea to contact station manufacturer to see what the latest firmware version is and upgrade as necessary)

6. The NIC Drivers have become corrupt
A: Update the specific Networking drivers in use on the MDC through the Device Manager in Windows

7. Turn off all power saving settings of the Ethernet Adapter in the device manager
A: Uncheck "Allow the computer to turn off this device to save power"

8. Check for Windows 10 update 1709 and 1803 as this update will not allow the NIC and Cellular Aircard to run simultaneously

A: Settings > Update and Security > Windows Update > “Update History” link – if there, see the steps in the FAQ 2949

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **AS SOON AS WE DOCK OUR MDC, WE LOSE CONNECTION TO THE WIRELESS.**
Q: **OUR WINDOWS 10 LAPTOP LOSES CONNECTION TO THE INTERNET WHEN THE NETWORK CABLE IS PLUGGED IN.**
Q: **OUR MDC HAS MICROSOFT VERSION 1709 OR 1803 AND CAN’T CONNECT TO WIFI WHEN DOCKED.**
A: Microsoft Updates (1709 and 1803) prevent the Wireless connection as soon as a Network cable is plugged into the device. This also occurs for MDCs/laptops that are docked (where the Network cable from the SX Processor is run through the docking station). As of January 2019, the steps to correct this are below.
WIN10 version 1803
1. Open Regedit
2. Expand HKEY_LOCAL_MACHINE
3. Navigate to Software > Policies > Microsoft > WcmSvc > Local
4. Right click on Local > Hover over New > Select “DWORD (32-bit)”
5. Name the new value “fMinimizeConnections”
6. Right click the on the new name > select Modify > Set value data to 1 (leave base Hex) > Click OK
7. Reboot Windows and test

WIN10 version 1709 - Microsoft fixed this with Update KB 4284822. But if you still have issues, the registry steps are below:
1. Open Regedit
2. Navigate to HKEY_LOCAL_MACHINE > Software > Policies > Microsoft > WcmSvc > Local
3. Right click on Local > Hover over New > Select “DWORD (32-bit)”
4. Name the new value “fMinimizeConnections”
5. Right click the on the new name > select Modify > Set value data to 0 (leave base Hex) > Click OK
6. Then Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Wcmsvc
7. Right click on Wcmsvc > Hover over New > Select DWORD (32-bit)
8. Name the value “IgnoreNonRoutableEthernet”
9. Right click on the new value > Modify > Set value data to 1 (leave base in Hex) > OK
10. Reboot Win10 and test

If the steps above did not resolve the issue, you may need to address this with Microsoft. Their support site is here.

APPENDIX D: XML DATASTREAM

Overview

The XML Datastream can be used to push the current data from a running PAGIS system to another application. The data available via the Datastream includes reads, hits and current images. The connection to the Datastream is a TCP/IP socket (default port: 10100). When initially connecting, an XML packet is passed to the PAGIS Software to subscribe to the Datastream. The data connection is configured as "push only" and doesn't allow receipt of additional external data. The current image stream is pushed periodically whereas reads and hits are passed as close to real-time as possible.

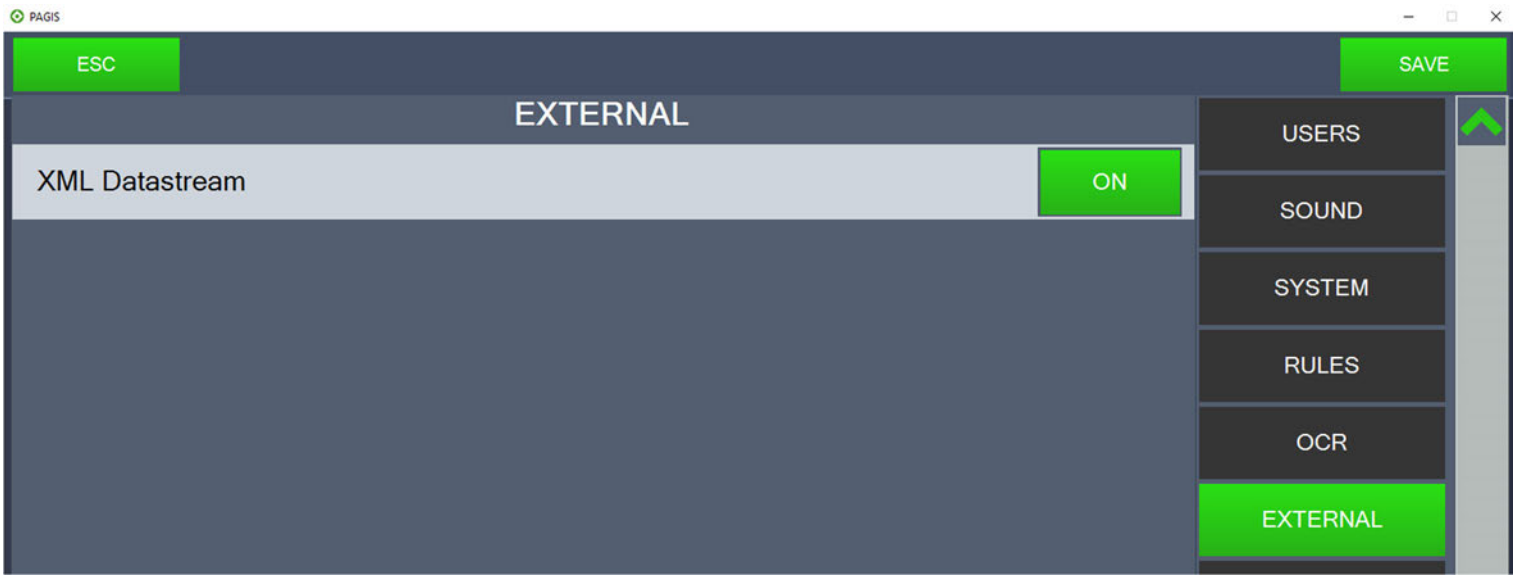
PAGIS Port

By default, the PAGIS.exe.config file has a key for defining the port number for the XML Datastream. The default value is 10100. This setting does not need to be changed unless the default port is unavailable.
The key has the following format:

```
<!--XML Datastream Settings/-->
<add key="XML.Datastream.Port" value="10100"/>
```

PAGIS Admin Setting

To utilize this feature, the XML Datastream needs to be enabled in PAGIS. To do this, navigate to Settings > Admin > External. The "XML Datastream" option should be turned on as shown in the image below and then saved.



XML Subscription

When initially connecting to PAGIS, the Datastream subscriber will receive only a Heartbeat XML packet (see example below) until PAGIS receives a subscription packet from the subscriber. The properly formed subscription packet defines the specific data that the subscriber wishes to receive.

Heartbeat XML Packet

The Heartbeat Packet is sent once every 10 seconds. The purpose of the heartbeat packet is to let the subscriber know that the communications channel is working between PAGIS and the subscriber. The timestamp is sent in the format of "`YYYY-MM-DDThh:mm:ss`".

Sample of the Subscription XML Packet

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-heartbeat>
  <timestamp>2011-10-13T09:41:56Z</timestamp>
</pips-datastream-heartbeat>
```

Subscription XML Packet

A properly formed subscription packet will have all of the data being requested from PAGIS. To receive a specific datatype, a tag must be added to the subscription to define the desired datatype. The valid entries for datatype are: Reads, Hits, and CurrentImage.

- Subscribing to Reads will send all plates that are detected by PAGIS regardless of whether or not it has an associated hit.
- Subscribing to Hits will send all plates detected by PAGIS that are on a hotlist and the associated Read data for that Hit.
- Subscribing to the CurrentImage Datastream offers two additional attributes that may be passed as well. The "camera" attribute can be set to determine which camera the image is coming from. If no value is passed for "camera" the value defaults to zero. The "milliseconds" attribute determines how long the system waits between sending the current image. The default value for milliseconds is 1000. If a value of zero is sent, the system will send a single snapshot.

Sample of the Subscription XML Packet

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-subscription>
  <datatype>Reads</datatype>
  <datatype>Hits</datatype>
  <datatype>HitTrigger</datatype>
  <datatype camera="0" milliseconds="1000">CurrentImage</datatype>
</pips-datastream-subscription>
```

HitTrigger

The HitTrigger packet is used to alert other systems that a hit has occurred on the PAGIS system. The packet is greatly simplified from the Reads/Hits XML packet and only contains the license plate text, timestamp and a description of the hit. The description will contain the name of the hotlist that originated the hit and may be used to send additional information.

Sample of the HitTrigger XML Packet

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-hittrigger>
  <timestamp>2011-10-13T09:41:56Z</timestamp>
  <vrm>SBX989</vrm>
  <hotList name='Alpha'>
    <field1><![CDATA[This is Alpha Field 1]]></field1>
    <field2><![CDATA[This is Alpha Field 2]]></field2>
    <field3><![CDATA[This is Alpha Field 3]]></field3>
    <field4><![CDATA[This is Alpha Field 4]]></field4>
    <field5><![CDATA[This is Alpha Field 5]]></field5>
  </hotList>
</pips-datastream-hittrigger>
```

Reads/Hits XML Packet

The Reads/Hits packet contains information about the plate that was detected. This information includes:

- Source – The device that detected the plate
- Camera – The camera on the device that detected the plate
- Read – The Information about the plate that was captured
- VRM – The plate translated to text
- Timestamp – When the read occurred
- GPS – The location coordinates where the read took place
- ImagesPatch – The image of plate in infrared (IR)
- Overview – The image of scene/car in Color
- Hits – The associated hotlist(s) data

Sample of the Current Image XML Packet

NOTE: The Current/Live Image XML Packet contains the current image from the camera. It is sent every 5 seconds.

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-currentimage>
  <timestamp>2011-10-13T09:41:56</timestamp>
  <data>(Image data here)</data>
</pips-datastream-currentimage>
```

2952

Sample Read with Hits XML

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-reads>
  <reads>
    <source>
      <name>PAGIS_90210</name>
      <software name="PAGIS" version="2.6.8" />
      <camera name="Front Left">
        <read>
          <state>TN</state>
          <vrm>SBX989</vrm>
          <confidence>97.5</confidence>
          <timestamp>2011-09-30T09:30:10Z</timestamp>
          <username><![CDATA[shronski]]></username>
          <gps>
            <latitude>-87.4567</latitude>
            <longitude>98.7654</longitude>
          </gps>
          <images>
            <image name='Patch'>
              <type>IR</type>
              <data>

<![CDATA[/9j/4AAQSkZJRgABAQAAAQABA.....................................................................
.....................................................................................................
..... /9k=]]>
              </data>
            </image>
            <image name='Overview'>
              <type>Color</type>
              <data>

<![CDATA[/9j/4AAQSkZJRgABAQAAAQABAAD..................................................................
.....................................................................................................
.... //2Q==]]>
              </data>
            </image>
          </images>
          <misread>0</misread>
          <manual>0</manual>
          <hits>
            <hotList name='Alpha'>
              <field1><![CDATA[This is Alpha Field 1]]></field1>
              <field2><![CDATA[This is Alpha Field 2]]></field2>
              <field3><![CDATA[This is Alpha Field 3]]></field3>
              <field4><![CDATA[This is Alpha Field 4]]></field4>
              <field5><![CDATA[This is Alpha Field 5]]></field5>
            </hotList>
            <hotList name='Beta'>
              <field1><![CDATA[This is Beta Field 1]]></field1>
              <field2><![CDATA[This is Beta Field 2]]></field2>
              <field3><![CDATA[This is Beta Field 3]]></field3>
              <field4><![CDATA[This is Beta Field 4]]></field4>
              <field5><![CDATA[This is Beta Field 5]]></field5>
            </hotList>
          </hits>
        </read>
      </camera>
    </source>
  </reads>
</pips-datastream-reads>
```


neology



PAGIS

Manual

Version 2.15

Updated 6/23/2022

Table of Contents

Table of Contents 2

NOTICES 4

Technical Support 4

Design Changes 4

Trademarks 4

Copyright 4

Version 4

INTRODUCTION 5

1.1 Dual Lens Color and Infrared Camera 5

1.1.1 Available Products 5

1.2 Using This Manual 6

SCREEN REFERENCE 7

2.1 The PAGIS Software Login Screen 7

2.1.1 Logging on with the Default Administrative Account 7

2.2 Main Screen - Live View 8

2.3 The PAGIS Navigation Buttons 10

2.3.2 GPS Indicators 11

2.3.3 PAGIS Status View 11

2.3.4 Day/Night Mode 12

2.3.5 Begin Shift / Download 12

2.3.6 Sync via USB Thumb drive (or Local Source) 12

2.3.7 Sync via Wireless Network 12

2.4 Cam Mode Button 13

2.5 Taking a Picture 13

2.6 Search Entry Screen 14

2.7 ADD Hotplates 16

2.8 The Review Screen 17

2.9 Reads 18

2.10 Hits Review 19

2.10.1 Set Disposition – Additional Detail 20

2.10.2 Add Notes – Additional Detail 20

2.10.3 Misreads 21

2.11 Audits 22

2.12 Targets 22

2.13 Databases 23

2.14 Databases Edit- “Manual Reports” 24

2.15 Software & Camera Firmware Update (Restricted Users) 25

ADMIN SETTINGS 26

3.1 Sync Options Screen 26

3.1.1 Synchronization to Disk 27

3.1.2 Synchronization with BOSS 28

3.1.3 Sync to “Instation” (Formerly BOF2 and BOF3) 29

3.2 PAGIS Privacy Settings (Local Data Retention) 30

3.3 Language 31

3.4 Location 31

3.5 Users 32

3.6 Sound 33

3.7 System 34

3.8 Rules 35

3.9 OCR 36

3.10 External 37

3.11 Cameras 38

3.12 Cameras Settings 39

3.13 Cam Setup 40

3.14 Configs (Camera View Modes) 41

3.15 Config Settings 42

3.16 Export Reads 43

3.17 Licenses 44

3.18 Info 44

3.19 Camera Firmware Update, (Admin) 45

3.19.1 PAGIS Software Update, (Admin) 46

PAGIS INSTALLATION GUIDE 47

4.1 PAGIS System Requirements 47

4.2 PAGIS Prerequisites 47

4.2.2 PAGIS Software Installation (MDC) 49

4.2.3 PAGIS Software Installation (Win10 Mobile Processor) 50

4.2.4 PAGIS Software Installation (Win7 Mobile Processor) 51

TROUBLESHOOTING TIPS _____ *52*

5.1 Troubleshooting & Tips _____ **52**

5.1.1 PAGIS with NetMotion VPN _____ **52**

5.1.2 Cisco VPN Client: _____ **52**

5.1.3 Microsoft .NET 4.5 or newer Installation _____ **52**

5.1.4 Firewall Settings for Client-Server Installations _____ **52**

PAGIS/BOSS4 CONFIGURATION _____ *53*

6.1 Creating a New Device in BOSS4 _____ **53**

6.2 Enabling a New Mobile System in BOSS4 _____ **53**

6.3 Assigning Ownership to a Device in BOSS4 _____ **53**

6.4 Assigning Hotlists to a Device in BOSS4 _____ **53**

APPENDIX A: THE GLOSSARY _____ *54*

APPENDIX B: PAGIS SOFTWARE DATABASE FILE _____ *55*

APPENDIX C: XML DATASTREAM _____ *57*

APPENDIX D: Hotlist API _____ *60*

API Hotlists Commands _____ *61*

1.1 GET Hotlists _____ **61**

1.2 POST Hotlists: _____ **62**

1.3 PUT Hotlists _____ **63**

1.4 GET Hotlist _____ **64**

1.5 PATCH Hotlist _____ **65**

1.6 Delete Hotlist _____ **66**

API Hotplate Commands _____ *67*

2.1 GET Hotplates _____ **67**

2.2 POST Hotplate _____ **68**

2.3 GET Hotplate _____ **69**

2.4 PATCH Hotplate _____ **70**

2.5 Delete Hotplate _____ **71**

2956

NOTICES

The information within this manual is authorized for distribution to customers, authorized service center personnel, and distributors of Neology. Every effort has been made to supply correct information. However, Neology assumes neither responsibility for its use, nor for any infringements of patents or other rights of third parties, which may result from its use. No license is granted by the manufacturer under any patent or patent rights. Neology reserves the right to modify and update the equipment at any time without prior notice. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means to a third party without the prior consent of the copyright holder. The manufacturer's warranty will be invalidated if untrained personnel operate the equipment or if any attempt is made to service the equipment by unauthorized personnel.

This manual contains confidential and proprietary information and should not be redistributed except as needed for proper use and maintenance of the agency's Mobile ALPR system.

Technical Support

Service of this equipment by replacement of parts, on-site repair, routine maintenance inspection, and scheduled remote support session is available. Please contact Neology ALPR Technical Support.
Phone: (833-747-7577), Option 2
USA Support Team Email: Alpr_support@neology.net
For Customers in Europe, Middle East and Africa: Support@PIPSTechnology.co.uk Web: https://neology.net
Fax: 858-391-0264
Corporate Office: 13520 Evening Creek Drive Suite 460. San Diego, CA 92128

Design Changes

Neology reserves the right to change the design of any product from time to time without notice and with no obligation to make corresponding changes in products previously manufactured.

Trademarks

Neology™ is a trademark of Neology Inc., and either registered or pending registrations in several jurisdictions. Windows, Windows 7, Windows 8, Window 10, and .NET are all trademarks of the Microsoft Corporation. Other trademarks and registered trademarks are the property of their respective owners.

Copyright

The Neology PAGIS Software is copyright of Neology. All rights reserved. This product contains confidential and trade secret information of Neology and is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portions of it, may result in civil and criminal penalties.

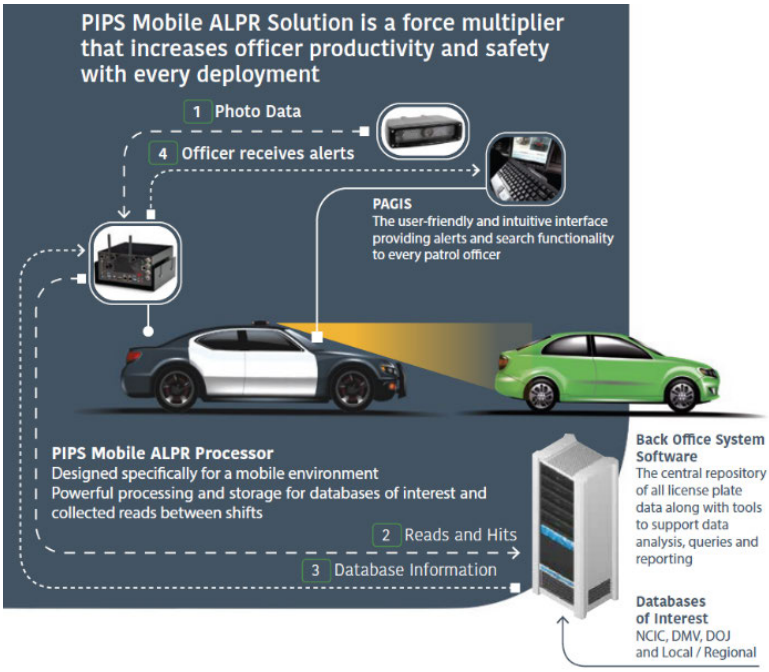
Version

This manual demonstrates the attributes of the Neology PAGIS Software Version 2.15.2.8 and was last updated in June 2022.

2957 INTRODUCTION

Neology's Automated License Plate Recognition (ALPR) software solution called PAGIS utilizes dual-channel, dual-lens, cameras to "read" plates. Our software is optimized to run on the Mobile Processor itself or in conjunction with a mobile data computer (MDC). Our mobile software is compatible with Microsoft Windows 7, 8, 10 and 11. The Mobile ANPR/ALPR Processor comes equipped with Microsoft Windows 10 Embedded.

The PAGIS Software processes the infrared plate image provided by any of the cameras and then interprets the plate number through Optical Character Recognition (OCR) via the mobile processor. The PAGIS application then searches for any matches of the plate with those listed in the databases, or "hotlists," distributed from the Back Office System Software (BOSS) or other external sources.



WARNING: **To reduce the risks associated with impact, which if not avoided, could result in serious injury or death: Do Not** interact with the ALPR system while driving in hazardous situations. The PIPS mobile camera series and License Plate Capture Software are not intended for use in hazardous environments, so that the User and/or others are not put at risk for personal injury and/or property damage.

1.1 Dual Lens Color and Infrared Camera

The Mobile ALPR System allows for a maximum of four (4) dual-lens cameras to be installed on each ALPR vehicle provided that the vehicle supports the additional mounting equipment.

Each dual-lens mobile camera uses visible light to take color overview pictures of the vehicle and uses infrared (IR) illumination to capture the license plate's alphanumeric characters. IR illumination offers the best capture performance of reflective license plate characters for the following reasons:

- State issued license plates are designed to be highly reflective to IR light.
- Cameras using IR capture technology do not depend on the presence of visible light to function.
- Cameras using IR capture technology are not negatively impacted by the effects of headlights, solar glare, or total darkness.
- IR light penetrates rain and fog better than visible light.
- Due to these attributes, the system can be used 24 hours a day, seven days a week.

1.1.1 **Available Products**

Additional information about this and other Neology applications, cameras, and solutions are available on the Neology web site: https://www.neology.net

2958

1.2 **Using This Manual**

The section overview of this software manual is as follows:

Section 1: The Introduction and Basics

Section 2: PAGIS User's Section: Explains screen function and User Operations in the PAGIS Software

Section 3: Software Administrator's Guide.

Section 4: PAGIS installation.

Section 5: Additional Information and Troubleshooting Tips

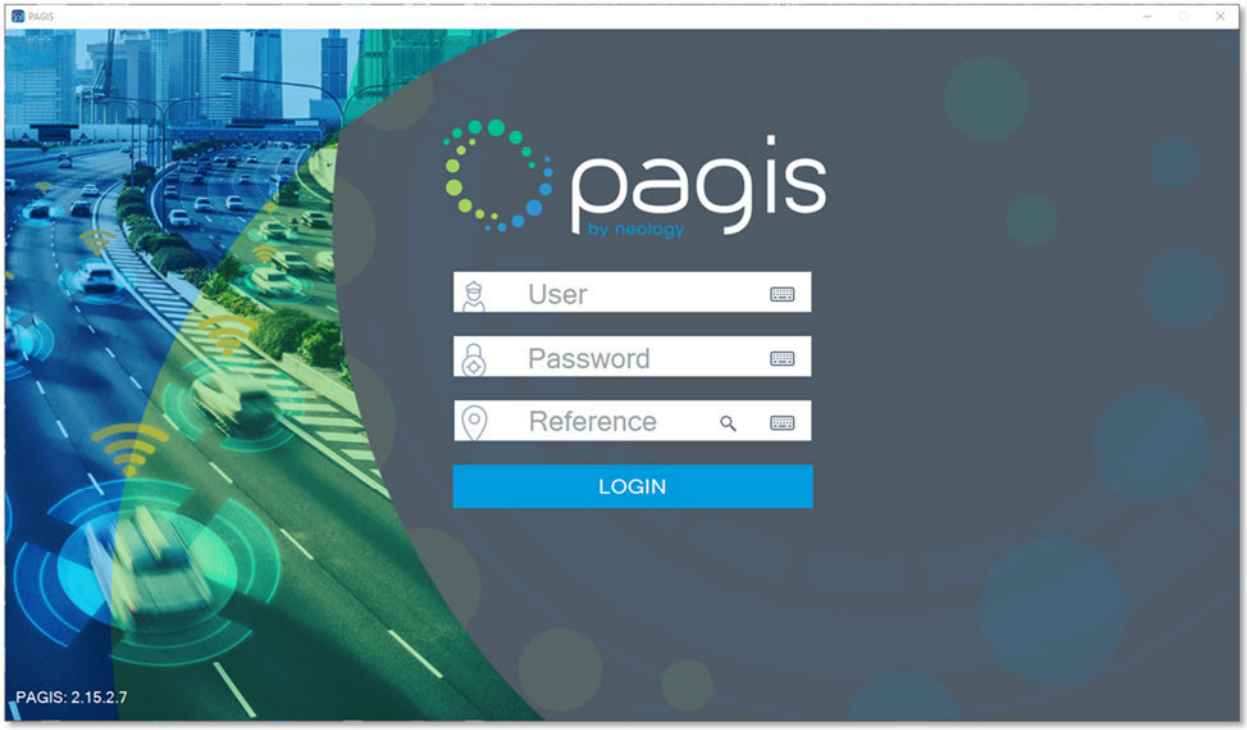
Section 6: Initial BOSS configuration for new PAGIS devices (MDCs)

Appendices: Additional features and details

2959

SCREEN REFERENCE

This section guides the user through the PAGIS Software screens and the available options. Screens are grouped according to function. When a button is grayed out or missing, the option is not available, or no information has been accrued to activate it.



2.1 The PAGIS Software Login Screen

The PAGIS Software allows users with various access privileges to use the same MDC. For users with touch screen monitors, the Keypad button immediately to the right of any text box gives the user access to an on-screen keyboard for data entry.

User Field: The alphanumeric string assigned to identify the user. Usernames are not case sensitive.
Password Field: Password of the assigned user logging in. Passwords are case sensitive.
Reference Field: This is an optional field utilized to fit several use cases. A user can manually enter a reference at logon, leave the field blank, or select list of unique tags that will be associated with all data captured while logged in. If the Administrator has configured a default reference tags, that information will be displayed automatically. Otherwise, it will be blank.
Login Button: Submits the username and password to attempt a login.

2.1.1 Logging on with the Default Administrative Account

The PAGIS Software includes a default administrative account that can be used for the initial configuration. To do so, simply click the Login button with the User and Password fields blank.

NOTE: System Administrators are strongly encouraged to configure users for PAGIS just before, or soon after the installation and setup. PAGIS users accounts are created and maintained in BOSS. Once Users are established by the BOSS System Administrator, the default user account is automatically disabled. Best practices are to be certain at least one User account has administrative privileges.

2960

2.2 Main Screen - Live View

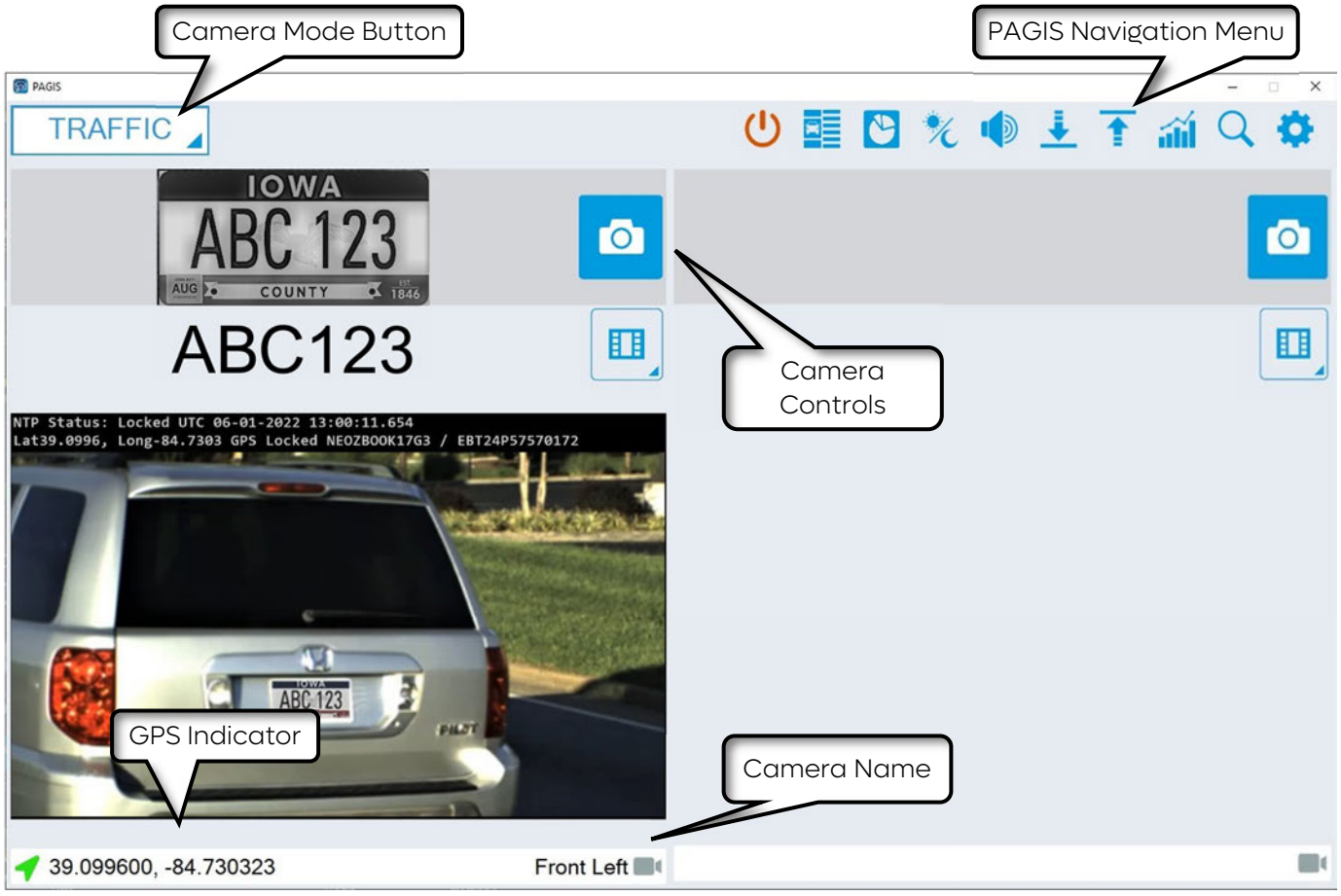
Upon a successful login, the user will see the Main screen (Live View). This is the default view and starting place of all PAGIS Software features. (NOTE: Access to features is based on user group rights established in BOSS.)

The Main Screen is also the place users will monitor read images and ALPR "hits". At the initial startup of the system, it is normal to see only a blank/grey screen for a few seconds. Once a connection has been established with the mobile cameras, white boxes will be displayed showing the live-feed camera panels. At this point, the system is ready to capture reads/plates.

PAGIS Dule Mode View

By default, PAGIS loads into a static view. This means live video will not automatically appear in the camera panels (white boxes) until a plate has been captured or the user selects one of the live feed options.

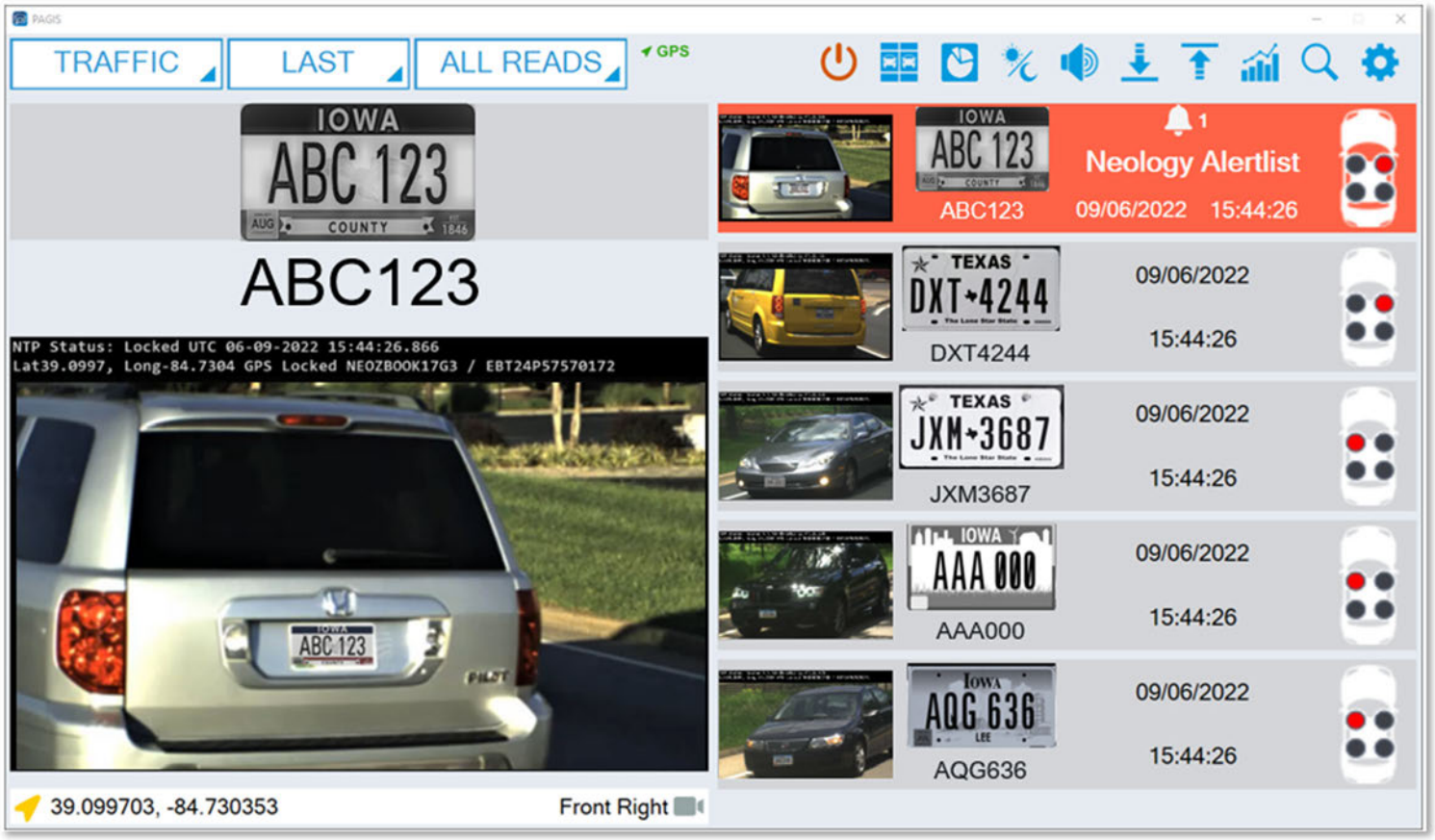
Once a plate is "seen" by a camera assigned to the current viewing mode (Traffic vs Parking), it will display the captured information in the corresponding camera panel. Each plate capture is also accompanied by a short "Beep" to audibly alert the user a read has taken place. (NOTE: If the user is in the Traffic Mode at the time a parking camera reads a plate, there will be a sound effect, but no plate image will be displayed on screen unless that plate is on a synchronized Hotlist or until the user switches to Parking Mode.)



2961

PAGIS Single Pane View

The single pane displays has one large active capture area on the left of the screen, this area will display all current captures in real-time, depending on Cam Mode selected. The panel on the right show you past captures and Hits, this area updates from the top down.

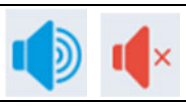


Single Pane Controls

- **Cam Mode:** Controls which cameras are active in the main display.
- **Last / Live:** Set the active capturer panel to static or live view. The Live mode alters the panel arrangement slightly, showing only the two primary cameras on the left without image patches.
- **All Reads / Hits:** Toggles to show only hits or reads in the history panel.

2.3 The PAGIS Navigation Buttons

This section provides a quick reference guide to the available navigation buttons of the Live View screen.

	The Camera Mode button is in the upper left corner and is used to switch between the configured camera modes. Once configured, the name will change to a selected mode. The default values are "ALL", "Traffic" and "Parking".
	**Logoff button:** When selected, the user will be logged out of PAGIS and return to the login screen. When Auto-login is enabled, this will close PAGIS.
	**Panel Mode:** Switch between Dule or Single panel modes in main live view screen.
	**System Status:** The system status screen provides an area where users can check on the available resources that effect PAGIS performance.
	**Sound button:** When selected, this will toggle the PAGIS Read capture sound On or Off, alert sounds will remain active.
	**Day/Nite mode:** Switch PAGIS between day & night mode screen skins.
	**Begin Shift / Download button:** Performs an BeginShift sequence that downloads Hotlist, Hotplate, Users credentials and targets from the Host. **End Shift / Upload button:** Performs an Endshift sequence that uploads captured Reads, Hits and PAGIS Audit information to the connected Host.
	**Statistics/Review button:** When selected the user can review Alert list, Reads, Hits, Targets, and other PAGIS information.
	**Search button:** Research all available Reads/Hits as well as manually add hotplates to PAGIS's local Hotlist list known as "Manual Reports".
	**Settings button:** Available to Users with administrator rights to modify PAGIS configurations.
	**Firmware & Software update:** This icon will appear when PAGIS detects a new software or camera firmware version is available. All user types are notified, but only Admins can apply the update.

Camera Control Buttons

The dual-lens cameras can capture both color and an infrared image. Formerly, there were a total of three buttons that allowed the user to view the IR and color feed as well as capture a picture directly from PAGIS. Now there is a toggle button to switch between color and IR views and a separate button to take a picture. These buttons are displayed on the main Live Screen as shown below.

	**The Camera View Selector button:** This is the default state at login showing the Static View. (NOTE: PAGIS does not automatically display a life feed.)
	**Color View:** by clicking on the Camera View Selector button once, the user will switch to the Color View Mode. This displays the current view of the color camera and will time out after 60 seconds.
	**IR View:** by clicking on the Camera View Selector button twice, the user will switch to the Infrared (IR) View Mode. This displays the current view of the IR camera and will time out after 60 seconds.
	**The Take Pic button:** Just above the Camera View Selector button is the "Take Pic" button. This button allows the user to quickly take a picture from the camera currently viewed.

2963

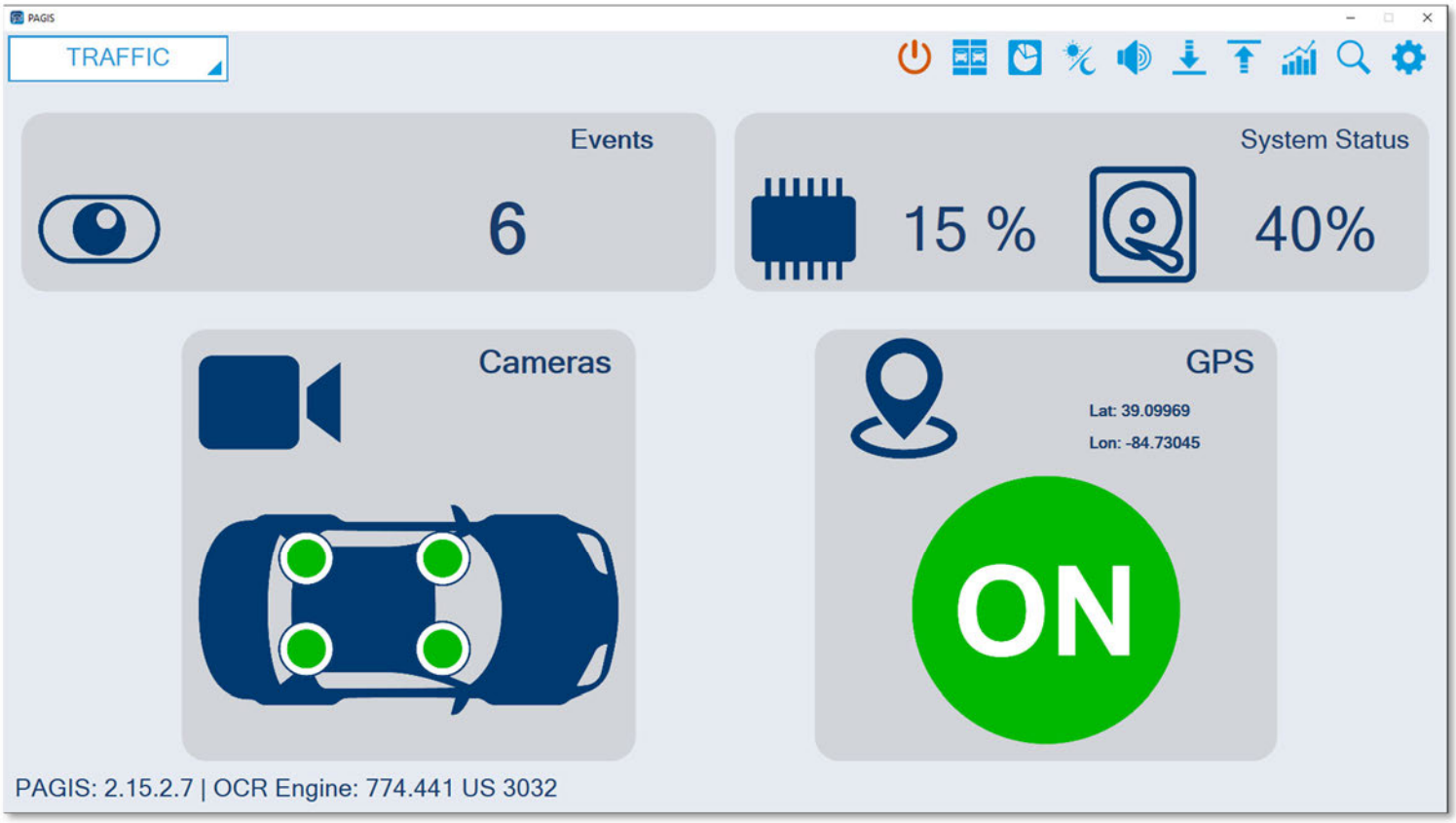
2.3.2 GPS Indicators

GPS is stamped on each read and hit as capture events take place by the system. The signal strength and location indicators are located underneath the camera panels at the bottom of the Live Screen.

39.341788,-84.298518 Shows an example of the Location Indicator displaying the Lat/Long on the most recent read
A green or yellow indicator shows a strong or medium strength GPS lock.
A red indicator shows there is no available GPS information.

2.3.3 PAGIS Status View

The status panel provides a means of monitoring key system resources in real-time important to PAGIS operations.



Status View Features

- **Events:** The events show the current number of captured plates in PAGIS.
- **System Status:** Displays the amount of RAM & DISK usage of the computer.
- **Cameras:** This indicates which cameras are active from the selected "CAM MODE".
- **GPS:** Displays if PAGIS currently has an active GPS signal. In Standalone mode the GPS area becomes clickable with the option to quickly change active COM ports for GPS communication.
- PAGIS and OCR Engine versions shown in bottom left.

2964

2.3.4 Day/Night Mode

Day/Night mode changes PAGIS user interface skins to a darker appearance to reduce illuminating the vehicle interior.



2.3.5 Begin Shift / Download

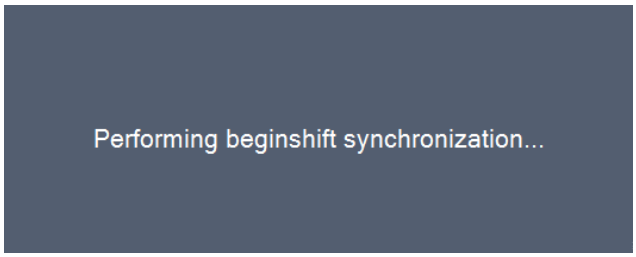
From the system menu, the PAGIS user can click the Begin Shift button . With most agencies, this action utilizes a cellular network to import all the necessary data used during a shift (Hotlists, Dispositions, and Targets) directly from the BOSS Server. However, agencies can also configure their systems to perform this function via Thumb drive or a local source file.

2.3.6 Sync via USB Thumb drive (or Local Source)

Depending on the agency network, some alter the default PAGIS/BOSS configuration mode to use a USB Thumb drive or locally stored file on the MDC/Laptop instead of the wireless Sync. To synchronize effectively, the user must first confirm he/she has access to the source location before initiating Begin Shift. NOTE: All synchronizations using this method must be performed manually.

2.3.7 Sync via Wireless Network

Synchronizations over a wireless network provide the agency with additional automated features. Best practices recommend the user manually launch Begin Shift from the Live View Screen at the beginning of every patrol shift. However, it is possible for users to allow PAGIS to synchronize via its auto-sync settings. When a manual Begin Shift is launched, the Main View Screen removes the camera feeds and displays a status window of the Sync process. Once the Begin Shift operation is complete, PAGIS will return to the normal Main View Screen.





2965

PAGIS Auto-Sync Settings

PAGIS auto-sync settings are best thought of as how PAGIS receives additional updates and maintains the downloaded ALPR data throughout the entire patrol shift. This prevents the need for the officer to manually perform Begin Shift functions multiple times a day. The auto-sync occurs every 10 seconds and receives data in small batches. The batches are not to exceed 1MB in size for every minute of download. In addition to receiving data, the auto-sync function also uploads a copy of data collected by PAGIS and sends it to BOSS.

Begin Shift – Additional information

By default, the synchronizations in PAGIS receive only what has been changed to the ALPR data since the last Sync. Meaning, if some plates have been removed from a Hotlist and others have been added, the system will only transfer that data instead of downloading the entire Hotlist each time the Begin Shift is launched. This helps to reduce the amount of data transferred over the agency's network. NOTE: Begin and End Shift synchronization, as well as all auto-sync features, are dependent upon stable communication to the BOSS server via an active data connection.

End Shift

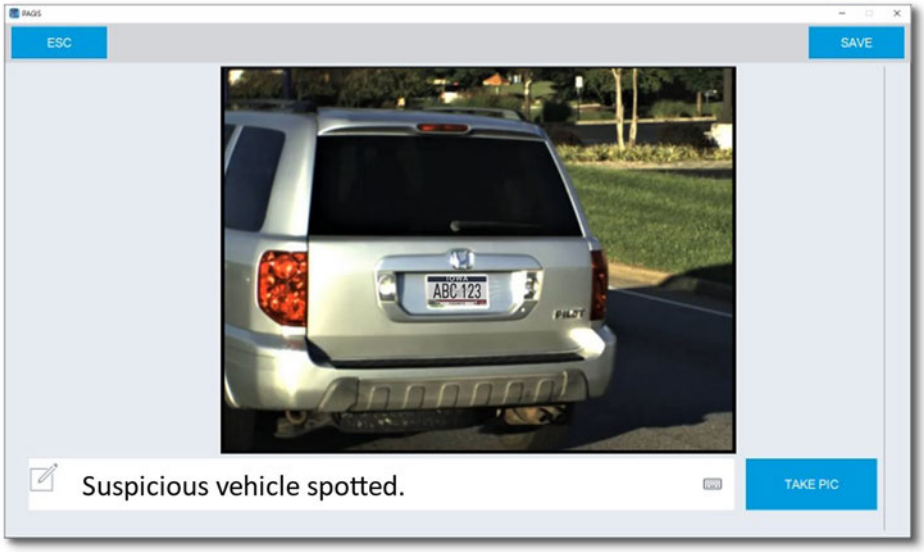
End Shift in PAGIS is the process in which all the collected ALPR data (Reads, Hits, and Images) from the recent shift is uploaded to the BOSS server and cleared from the local cache. As with Begin Shift, the agency has two options. They can choose to Sync via USB Thumb drive or via wireless connection. Best practices recommend users perform an End Shift Sync at the end of every patrol unless the "Privacy" setting is enabled, in this case the End Shift action is not required as PAGIS will purge locally stored data based on the privacy schedule. During the Sync, PAGIS uploads any Reads, Hits, and Images not already synchronized to BOSS and purges these items from the local cache on the MDC's hard drive. Completing an End Shift also removes any VLP entries manually added to PAGIS during the shift.

2.4 Cam Mode Button

Clicking the Cam Mode button in the upper left corner of the Live View Screen allows the user to cycle through the different camera modes configured by the PAGIS Administrator. Changing the camera mode changes which cameras are displayed on the Main Screen. By default, PAGIS provides "Parking" and "Traffic" as the two configuration modes. Users often switch these modes to suit their current use-case. For example, an officer in a parking lot will often switch the mode to "Parking" so s/he can see the parking cameras on the Live View Screen. They can then switch back to "Traffic" when monitoring city streets.

2.5 Taking a Picture

The PAGIS software has ability to quickly take a picture from one of the currently displayed ALPR cameras on the Live Screen. The user only needs to click on the Take Pic button.



2966

To Take a Picture:

1. From the Live View Screen, press the Take Pic button from the desired camera
2. The image taken will be displayed
3. Enter a description of the picture in the text field at the bottom of the screen
4. Press Save to save the picture or escape to cancel. Either action will return you to Live View.

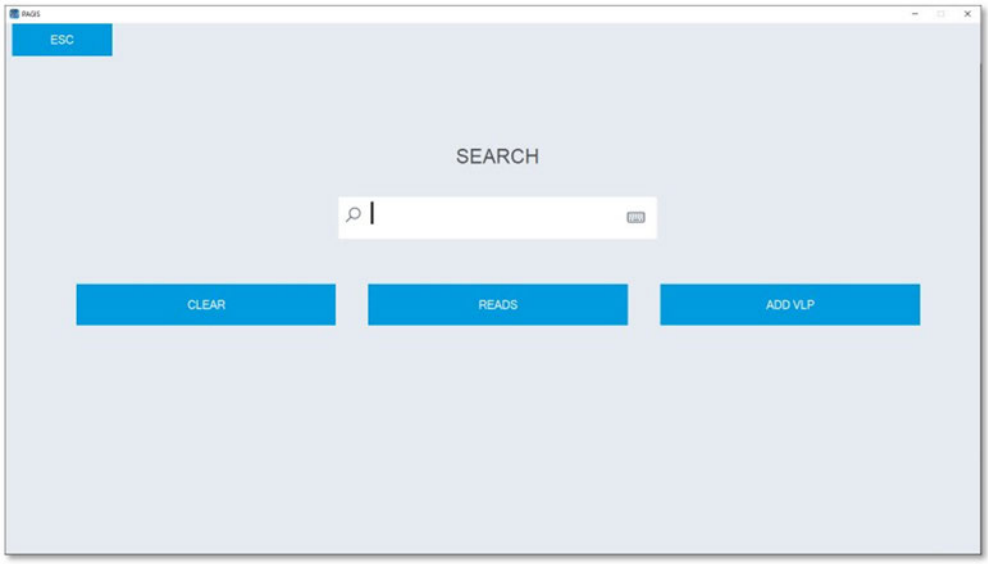
NOTE: The picture will not be saved if a description/note is not entered in the text box.

To View the Saved Images:

1. Navigate to the Review menu in PAGIS
2. Select Audits
3. The user will be able to see a thumbnail of the image and the saved text/note
4. To review the saved images later, the user will need to run the Audit Images Report from BOSS.

2.6 Search Entry Screen

Pressing the Search button icon from the Live View screen or Search from the Databases window allows the user to search all manually entered plates as well as all BOSS synchronized databases (Hotlists) for license plate and target information. Users can also search all locally stored reads/images accrued since the last End Shift by clicking the Reads button instead of pressing the Enter key.



Search Box: The text field used to enter the desired plate search via alphanumeric characters and/or wild card symbols, acceptable wildcards are the Asterisk * and Underscore _.
Clear Button: Clears the contents of the search box.
Reads Button: This button searches for a match from all the reads/hits locally stored in PAGIS.
ADD VLP: Searches all locally stored hotlists for the plate and if there's no match, allows the user to add the plate to the "Manual Reports" alert list for use in the field. NOTE: Wildcards are not permitted when using "ADD VLP".
ESC: The Escape button allows the user to exit to the Main/ Live View screen.

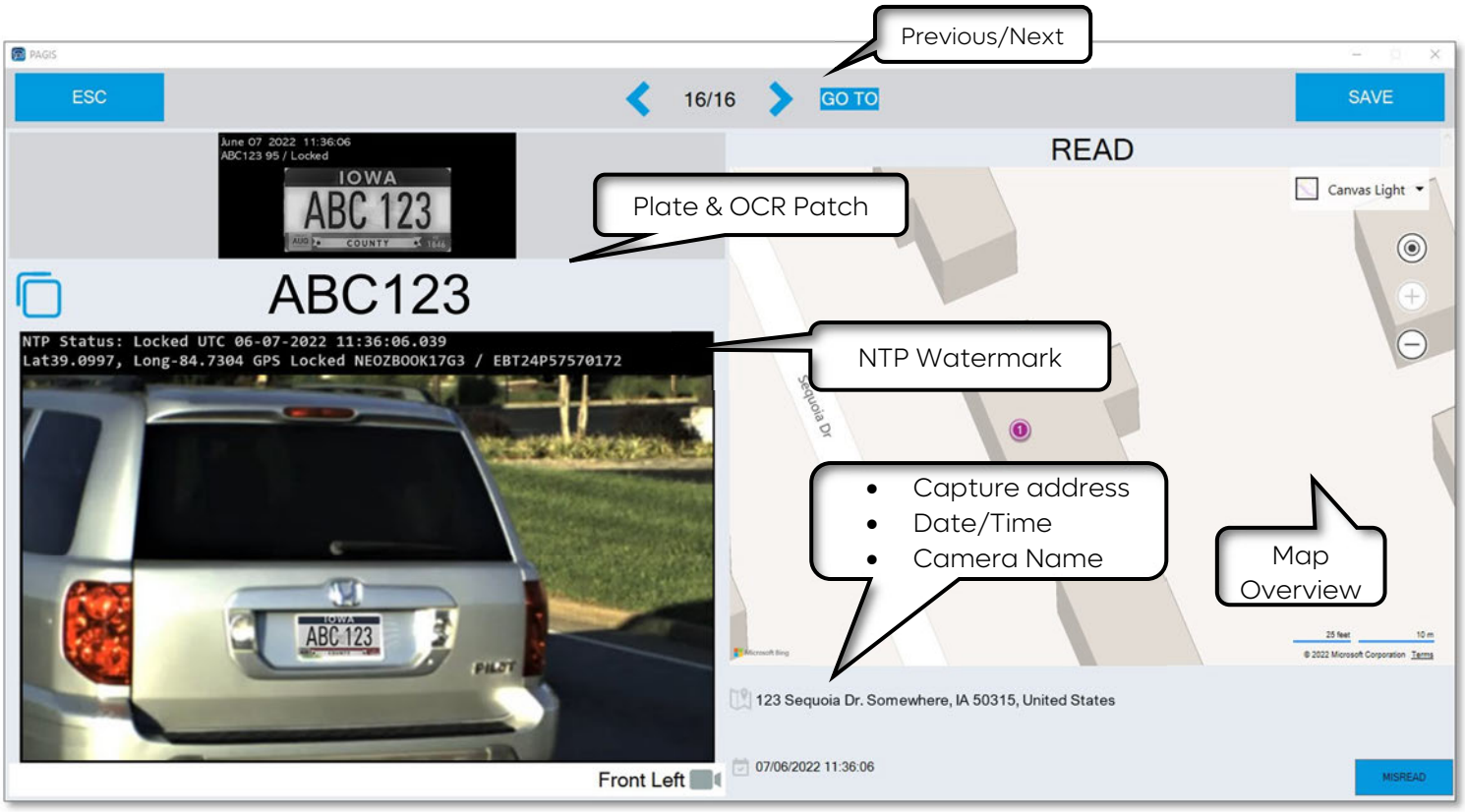
2967

Searching Locally Stored Reads and Hits

As mentioned previously, this search function allows users to find reads and hits directly from their recent patrols using the search field and the Reads button. These searches only apply to reads and hits locally gathered/stored in PAGIS that have not been purged due to Endshift or by the privacy purge schedule.

Searching for a Match

- From the Search field, users may enter a plate (or partial plate with wildcards) and then click the READS button.
- Results are displayed with the data gathered at the time the read was taken (See example below).
- Each result should display the infrared (IR) image of the plate as well as the color overlay of the vehicle along with the NTP status watermark.
- Each result shows the GPS data, Closest address point, Time and Date, and the Camera that read the plate.
- If there are multiple results, the user can cycle through them by clicking the left and right navigation arrows.



Wild Card Symbols

The use of wild card symbols in the Search box allows greater flexibility for the user, but may return a larger set of results.
Wild card searches performed using the asterisk (*) designates an unknown number of characters.
Wild card searches performed using the underscore (_) indicates a single missing or unknown character.
Searches can be performed using one, both or no wild card symbols.

Example: The officer received an alert from Dispatch looking for a vehicle plate containing the letter J and the number 8 separated by one character. Because the officer doesn't know how many characters there are before or after the J and 8, he enters *J_8* in the search box to review all possible matches of J and 8 separated by only one digit.

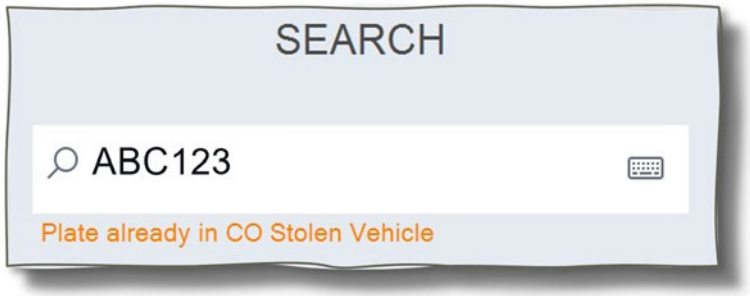
2968

2.7 ADD Hotplates

PAGIS allows users to manually add a plate of interest directly into the software as needed. Once saved, these entries are stored as part of the Manual Reports Hotlist and work just like any other Hotlist synchronized from the BOSS server, however this local Manual Report hotlist is isolated to PAGIS, and dose not transfer to BOSS or any other mobile systems. These hotplate additions are designed to be temporary and are cleared from the software with each End Shift.

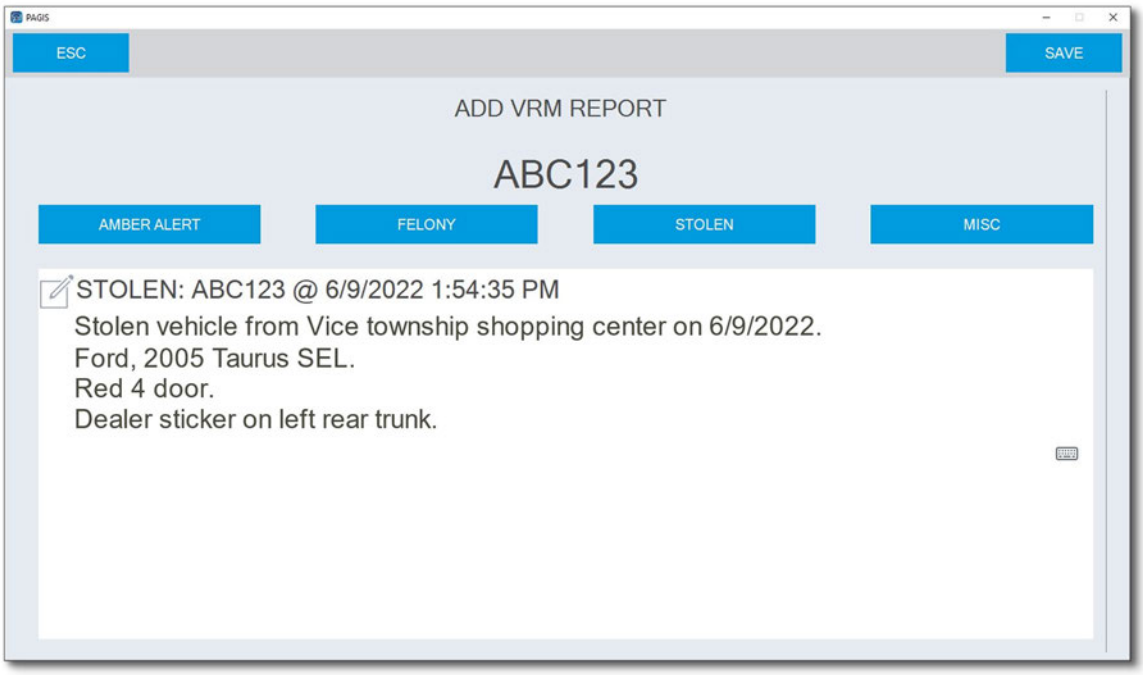
ADD VLP Query

Before an entry is added to the Manual Reports Hotlist in PAGIS, the software searches all stored databases for a match. If a match occurs, a message will display under the search box showing which Hotlist(s) it has been found in. If the VLP query does not return a match, the "ADD VRM REPORT" screen appears.



ADD VRM Report Screen

If the desired plate does not already reside in another Hotlist, the ADD VRM Report Screen becomes accessible.

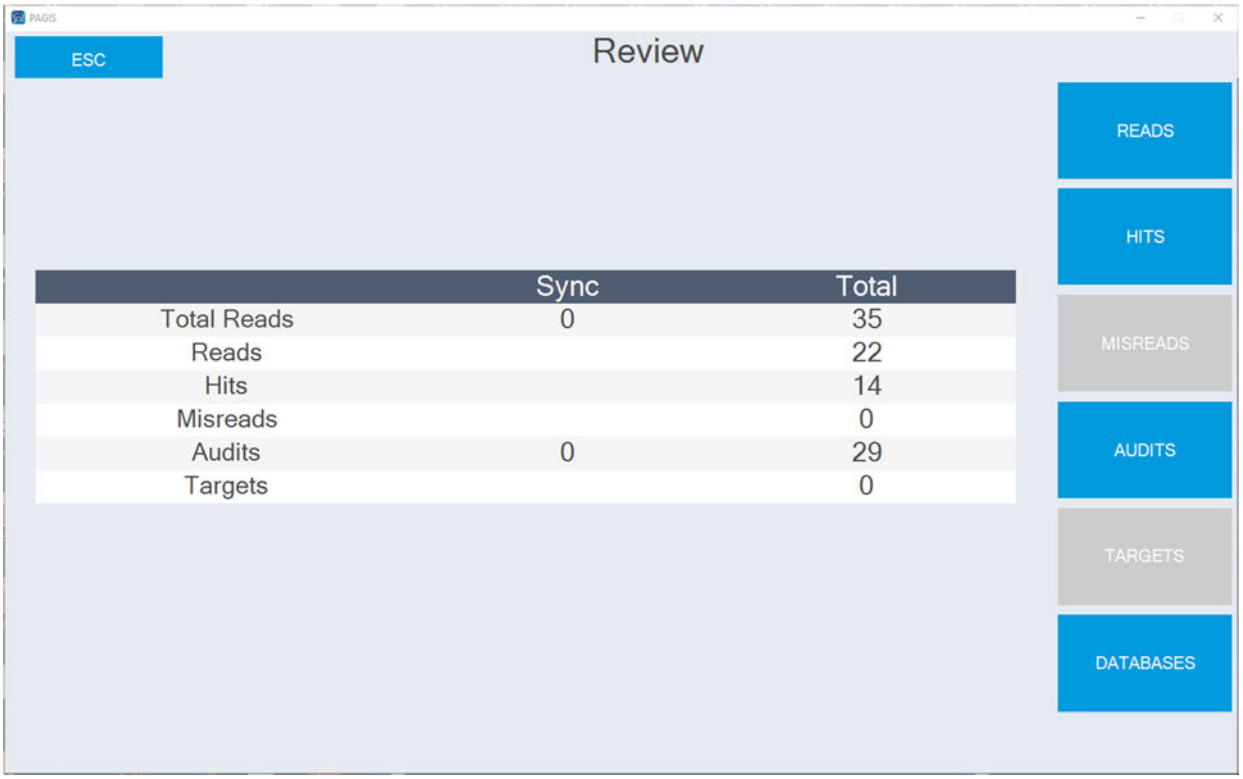


1. From the Search Entry Screen, enter the desired plate to add.
2. Click the ADD VLP button. If no match is found on any other hotlist, the "Add VRM Report" screen will appear.
3. Click to select the applicable alert type (AMBER ALERT, FELONY, STOLEN or MISC)
4. Either leave the default information or add additional detail by typing in the text filed below.
5. Click SAVE at the top right to add the plate to the Manual Entries Hotlist.

2969

2.8 The Review Screen

PAGIS allows users to review all locally stored data from one easy location. Clicking the Review icon from the Main Screen launches Review. This screen is divided into the Summary View Chart and sub-section navigation buttons to the right.



Summary Review Section

The Summary View Chart is divided into five categories and allows a user to review the information collected during their shift.

Total Reads: Shows the total number of Reads/Hits synced to BOSS and the total number of reads captured.
Reads: Shows the total number of reads only captured.
Hits: Shows the total number Hits captured.
Misreads: Shows the total number of Reads/Hits marked as a "misread".
Audits: Shows the total number of audits synced to BOSS and the total number of audits during the shift.
Targets: Shows only the number of targets downloaded from BOSS.
(NOTE: The Sync value will always be zero for customers using Disk Sync mode/Client Tools.)

Review Navigation Buttons

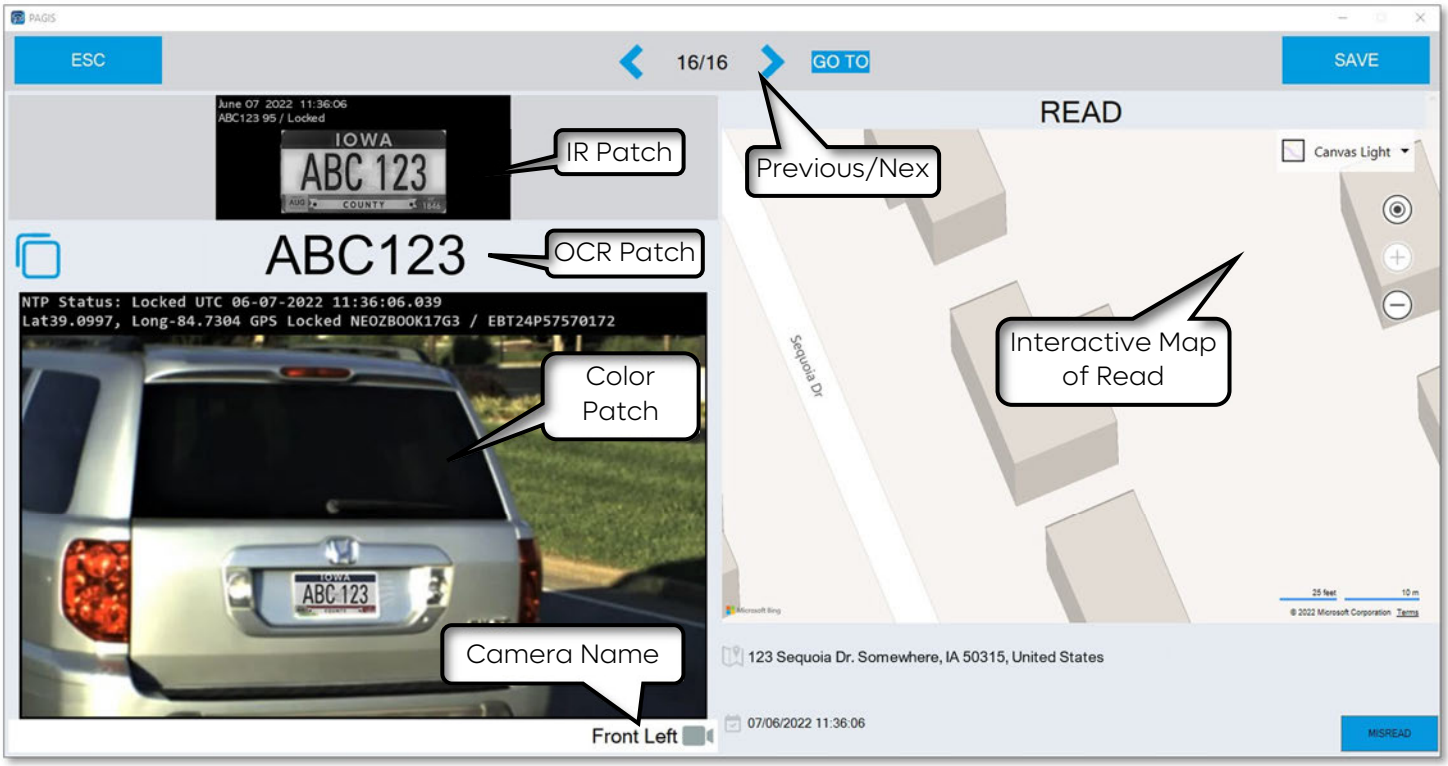
The navigation buttons allow the user to review specific sets of information gathered during the shift.

Reads: Review all plate detections that have occurred since the last End Shift synchronization.
Hits: Review the hits that matched a Hotlist.
Misreads: Review reads and/or hits that have been manually flagged as misreads, where the plate number in the image does not match the OCR interpretation of the plate (e.g., a letter O misread as a Q or zero).
Audits: Review failed and successful logons, any manual data entered during the shift, pictures taken and all manual license plate searches.
Targets: Review targets that have been synchronized from BOSS.
Databases: Review all the Hotlists currently distributed to PAGIS.
Esc: Returns the user to the previous screen.

2970

2.9 Reads

The Read Review Screen is divided into two main sections. The left side displays the information gathered at the time of the read and the right side displays an interactive map of the GPS location.



NOTE: Buttons that are greyed out indicate options that are not available in the current view. For example, the Reads and Hits review screens share the same layout but different on-screen options.

Interactive Buttons – Reads Screen

From the Reads Review, the user can interact with the following:

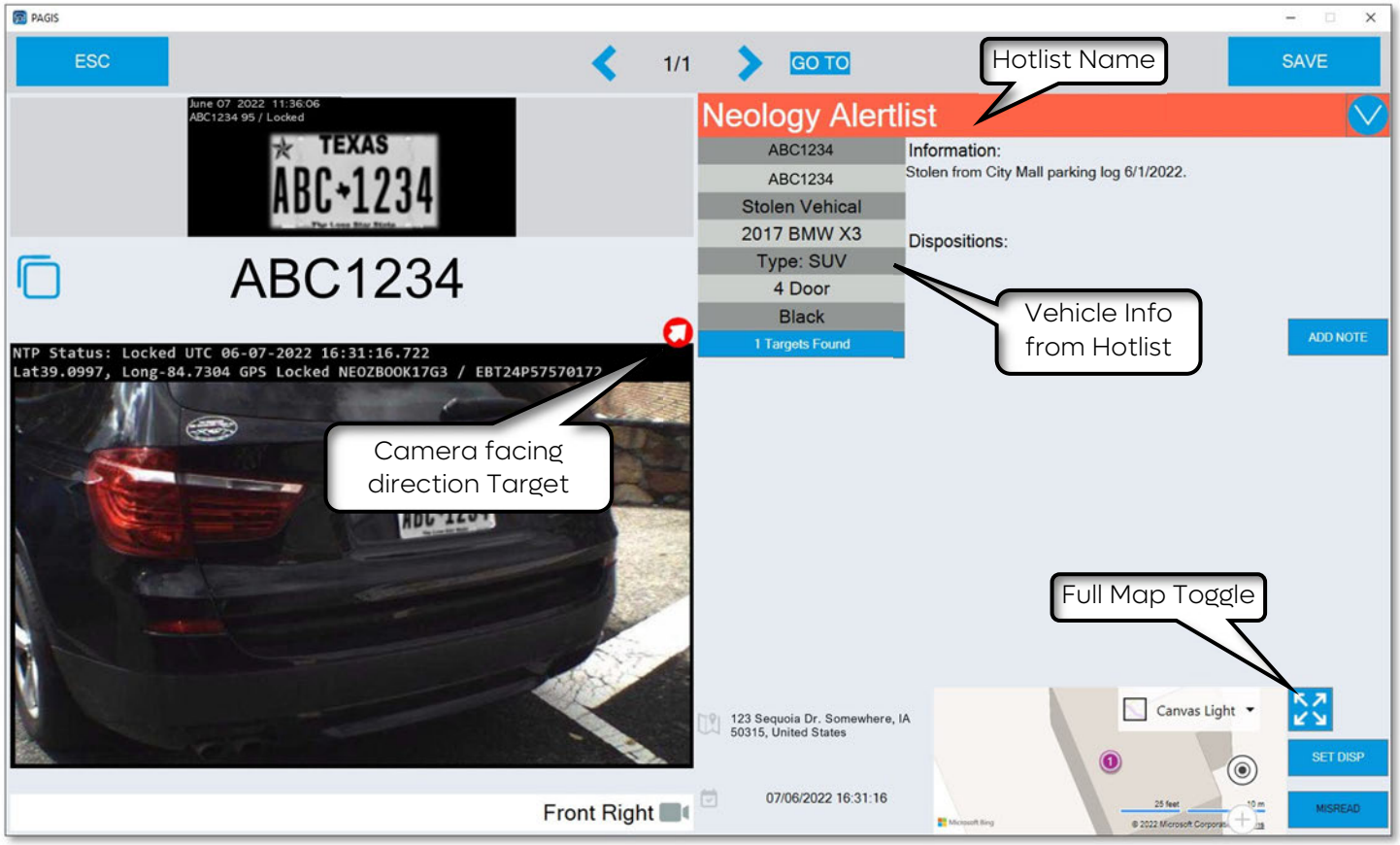
- **IR Patch:** The user can click on the IR "Patch" plate image to open a full-screen view.
- **OCR Patch:** The user can click on the OCR "Patch" image to edit the license plate number if necessary/Misread.
- **Color OV Image:** The user can click on the color image to open a full-screen view.
- **Map:** The user can manipulate the interactive map of the read location (Map Type, Scroll, and Zoom).
- **Misread:** Tags the event as a misread without correcting the plate number.

2971

2.10 Hits Review

Users can manually access the Hits Section by clicking the Hits Button from the review screen. The Hits Screen is also divided into two main sections. The left side displays the information gathered from the ALPR equipment during the read. And the right side displays the information provided by the associated alert list.

NOTE: Each time a VLP matches a Database value (a license plate read by the system matches a Hotlist entry), PAGIS plays an audible tone and automatically displays the Hit Screen to alert the user, however the popup behavior can be disabled by a system administrator.

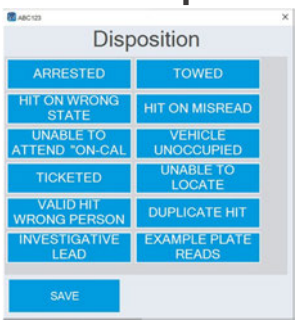


Hit Screen Attributes

Hit Count and Navigation Buttons: Displays the total Hits from this plate as well as the Next/Previous navigation buttons to view other hits this plate registered against.
IR Patch Image: The user can click on the IR "Patch" plate image to open a full-screen view.
OCR Text: The user can click on the OCR "Patch" image to edit the license plate number if necessary/Misread.
NTP Watermark: The NTP watermark allows for a confirmed GPS time/date stamp to be applied to the digital photos taken by the mobile cameras at the time of capturer, this applies to both the IR and Color patch images. The watermark helps to confirm the captures authenticity if a time/date discrepancy should arise among the various equipment platforms that make up the mobile ALPR system.
Overview Image: The user can click on the color image to open a full-screen view.
Camera Name: The name of the camera that captured the hit.
Hotlist Name: This is the name of the Hotlist or "Database" where the plate was matched.
Target Button: When available, this indicates a person of interest is associated with the Hit.
Vehicle Information: The area of grey bars will display the related vehicle information from the Hotlist. Any information added manually by the user will appear in the Text Box near the bottom of the screen.
Interactive Map: Shows a map location the Hit took place. Users can access full-screen view by clicking the expand map button.

2972

2.10.1 Set Disposition – Additional Detail

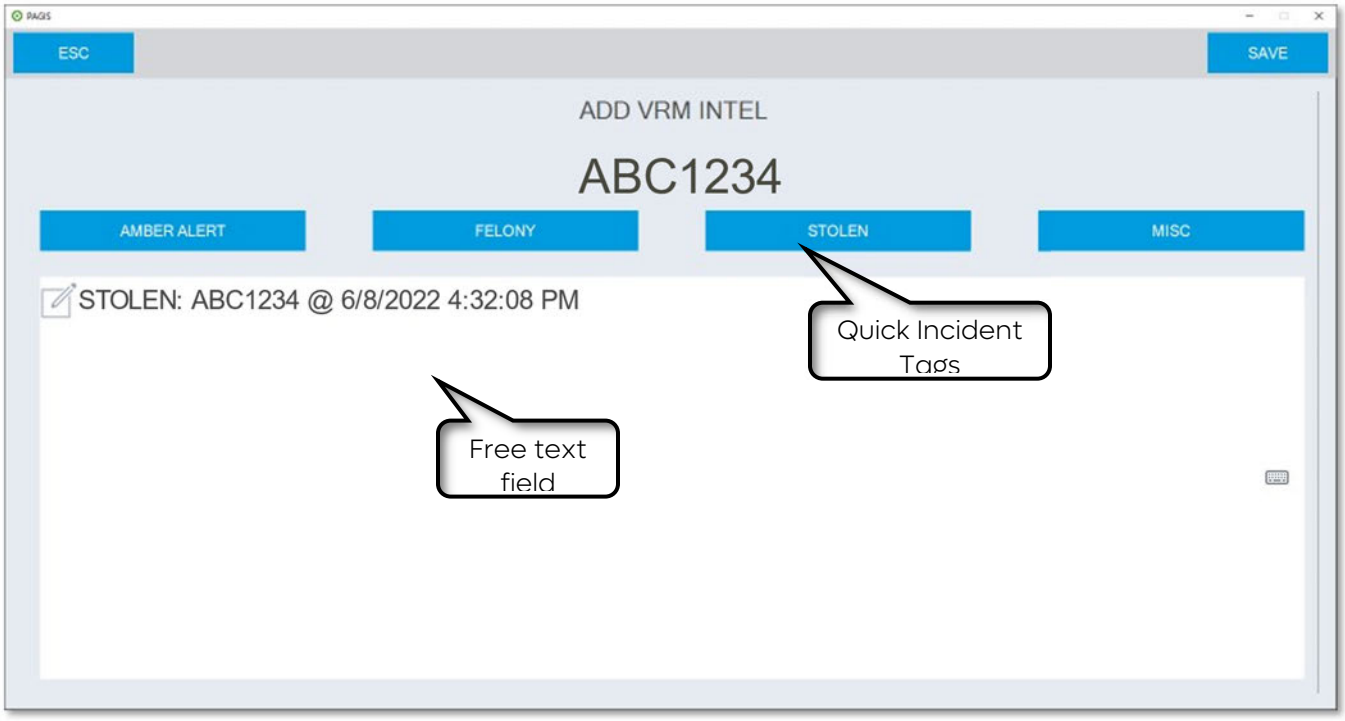


PAGIS allows for additional information to be added to a record in the form of a Disposition. Once Hits are flagged with a disposition code, the Agency can run a "Reads Statistics by Disposition Report" in BOSS. Thus, providing valuable metrics and understanding to leadership regarding their ALPR Enterprise.

When the "Set Disp" button is selected, the user is prompted to choose from a list of predefined values set by the Agency/BOSS Administrator. Once a disposition is selected and saved, the disposition is reported to BOSS and will also show up in the Hits Review Screen text box in PAGIS on the next alert notification.

2.10.2 Add Notes – Additional Detail

The Add Note button launches the Intel screen. The user is prompted to assign one of four values: Towed, Arrest, Not Recovered, and Misc. by clicking the associated button at the top of the screen. The user may also enter additional detail regarding the license plate/vehicle. After clicking the Save button, the intel will now appear in the Hits Screen text box.

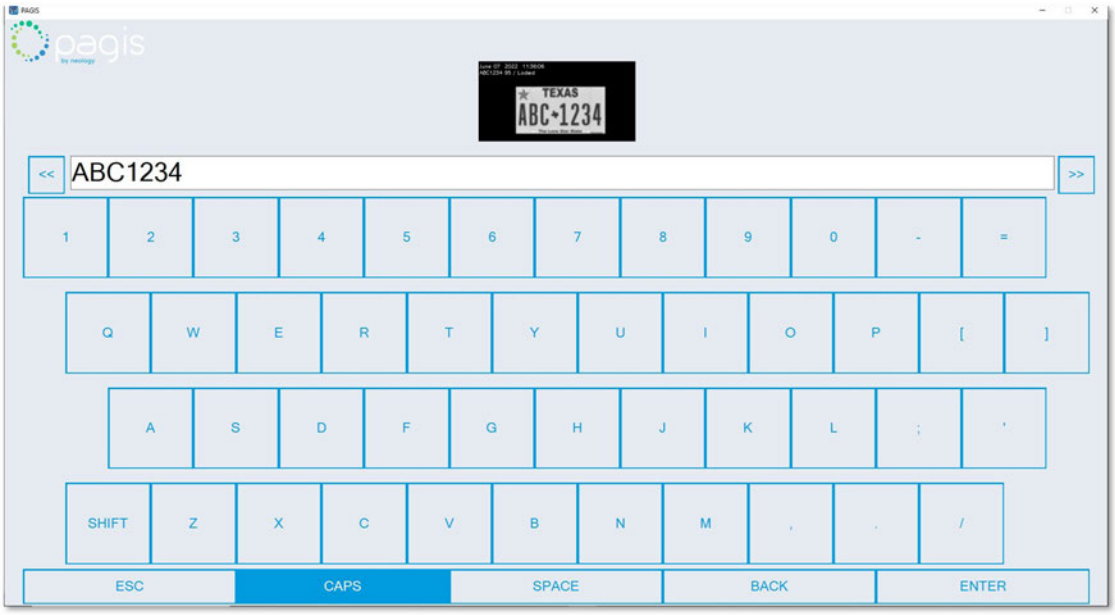


2973

2.10.3 Misreads

PAGIS allows the user to mark Reads and Hits with incorrect OCR translations as a Misread. This is most done by Agencies for Hits as users typically don't have time to review every single Read. Once an errant Hit is corrected, the system updates the record to show it as a Misread and will demote a registered hit as a misread, thus improves Agency Hit Reporting.

Correcting a plate read can be accomplished by clicking on the "OCR Patch" in either the Hits or Reads review screen. When the user clicks on the OCR Patch, the OCR Edit Screen opens and allows the user to update the Vehicle License Plate (VLP) data.



Marking a Record as a Misread:

The user can mark a record as a Misread from both Reads or Hits Review Screen. Each user can either simply flag the record as a Misread or update the OCR Patch information. NOTE: This ability is only available until the user has performed an End Shift function.

Manually Flagging a Read or Hit as a Misread:

1. Navigate to either the Reads or Hits Review Screen
2. Click on the Misread button on the Right
3. Click Save
4. Take note that the record title has now changed from "Read" to "Misread"

Updating the Read/Hit OCR Patch:

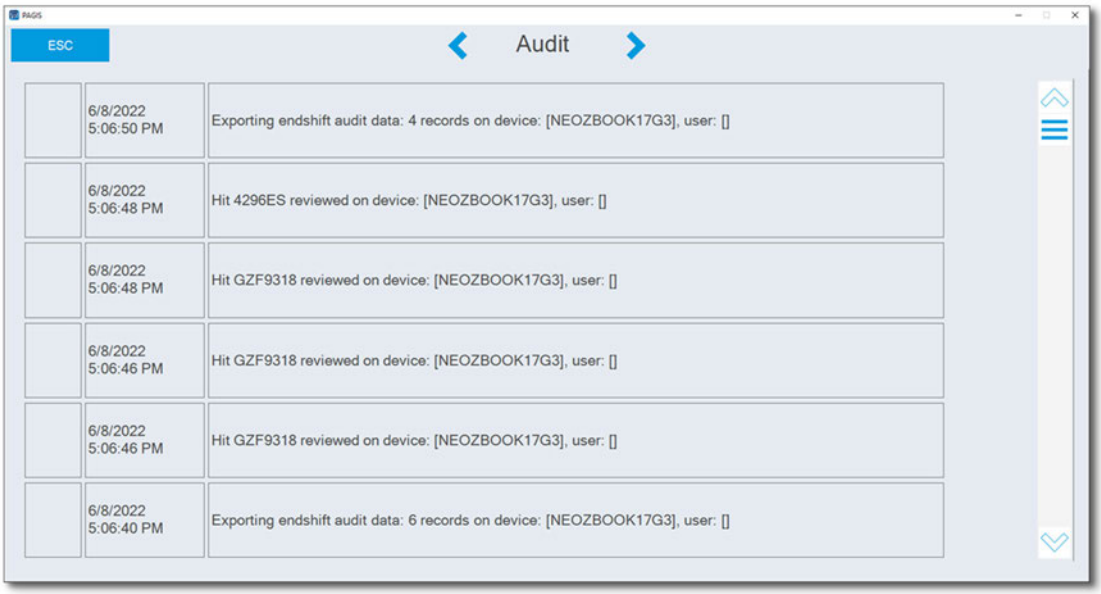
1. Navigate to either the Reads or Hits Review Screen
2. Click on the OCR Patch (Text just under the IR Plate Image)
3. Use the keyboard or on-screen keypad to update the Vehicle License Plate Number
4. Click the Enter Button to Save the changes (and exit back to the Review Screen)
5. When the user saves the changes to the OCR Patch, the record (Read/Hit) is automatically flagged as a Misread

2974

2.11 Audits

PAGIS logs both user and key system activity during each use of the software. The audit log captures various information like Read searches, synchronizations, hits, and user login attempts. The Audit Report is viewed in PAGIS by navigating to the Review section and selecting AUDITS.

NOTE: Performing an End Shift or syncing the database clears the current log.



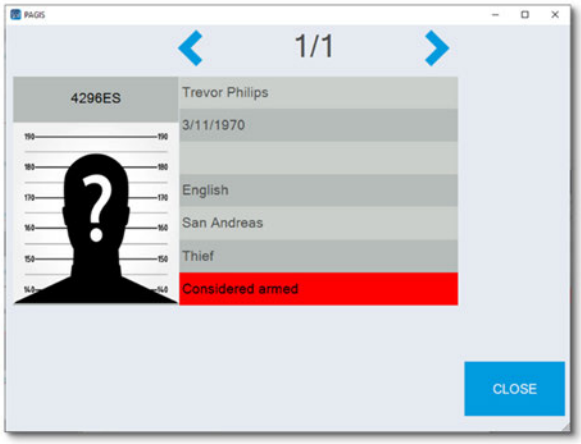
2.12 Targets

PAGIS can display information regarding Persons of Interest in response to a Hit alert. Targets are created by BOSS/Hotlist Administrators, and typically provide detailed information about owners of a registered vehicles. When configured, Target data is always linked to unique VLP data (a specific License Plate). If PAGIS registers a Hit on a Plate with a target ID, the Target Information Button is displayed in the Hit Alert window and allows the user to access the Target Screen.



The Targets Screen

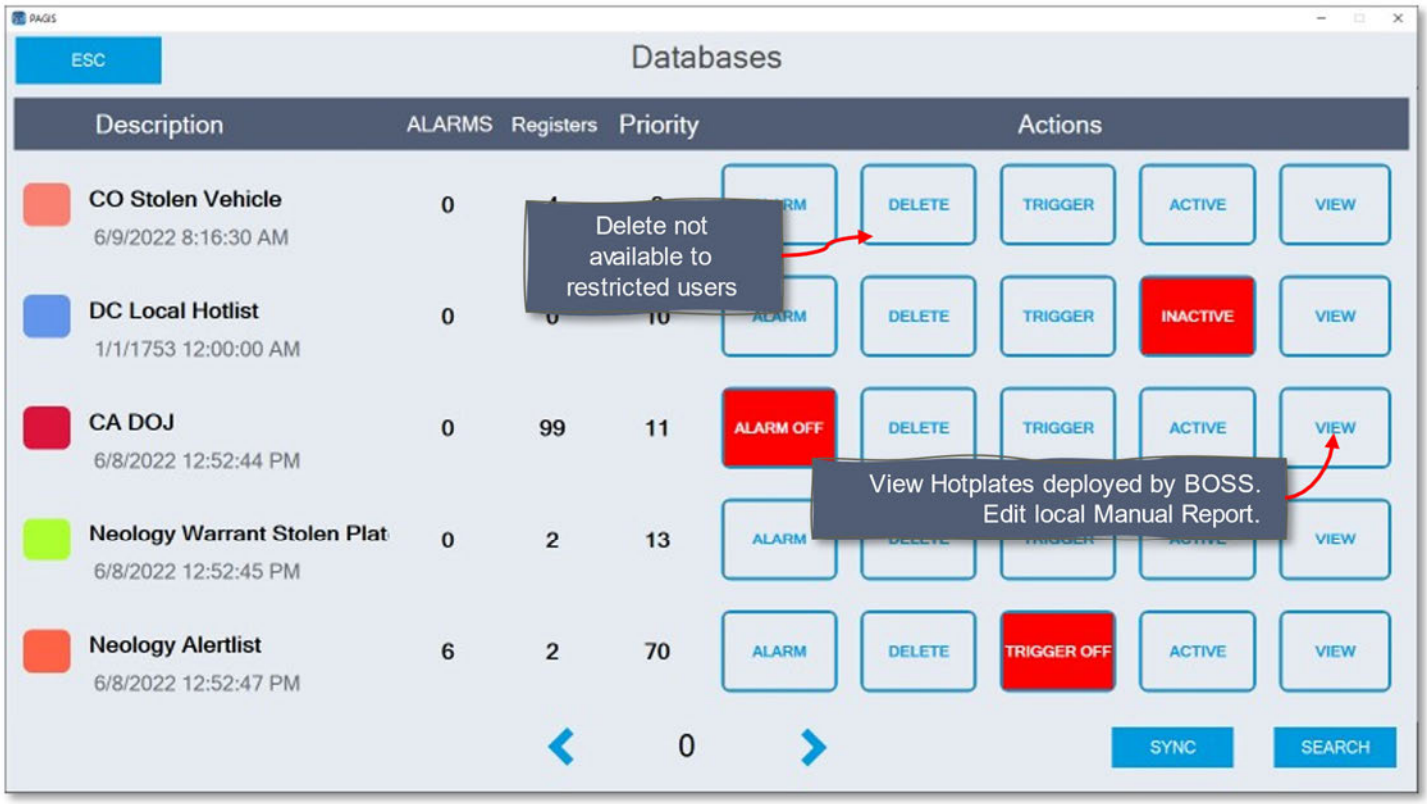
When a PAGIS user clicks the Targets Found Button from a Hit, the Targets Screen opens. This screen displays the information from the BOSS server about the Person(s) of Interest matched to the Hit.



2975

2.13 Databases

Users can review Hotlists in PAGIS by navigating to the Review section and selecting DATABASES button on the right. From the Databases Screen, users can toggle Hotlists functions such as disabling alters .



Databases Functions

Hotlist Color Code: The color attributed to each Hotlist by the BOSS Administrator.
Hotlist Name: The name of the Hotlist given by the BOSS Administrator. Also shows the time/date of the last updated.
Alarms: Indicated the number of hits currently assiated with a hotlist, this only pertains to data stored in PAGIS.
Registers: Indicated the number of hotplate in a hotlist.
Priority: The priority of the Hotlist assigned by the BOSS Administrator. The lower the number between 1 and 999, the higher the priority. If a plate resides on multiple Hotlists, the list with the higher priority will be displayed first.
Alarm Button: Toggles audible alerts On and Off for each Hotlist until the next synchronization.
Delete Button: Based on user rights, allows the user to temporarily delete a Hotlist from PAGIS until the next synchronization with exception of the Manual Reports. Click delete button to confrim, then save to apply.
Trigger Button: Toggles external triggers On and Off. An example of an external trigger is a light bar.
Active Button: Disables and enables each Hotlist (each Hotlist is set to On by default).
View: View and edit localy created hotplates with a given hotlist, Hotlist/Hotplates deployed via BOSS can only be viewed.
SYNC button: Synchronizes PAGIS with the BOSS server to update the Hotlists.
SEARCH button: Open the Search Entry Screen (See section 2.8 for more information).
< >: View previous and next page of hotlist.

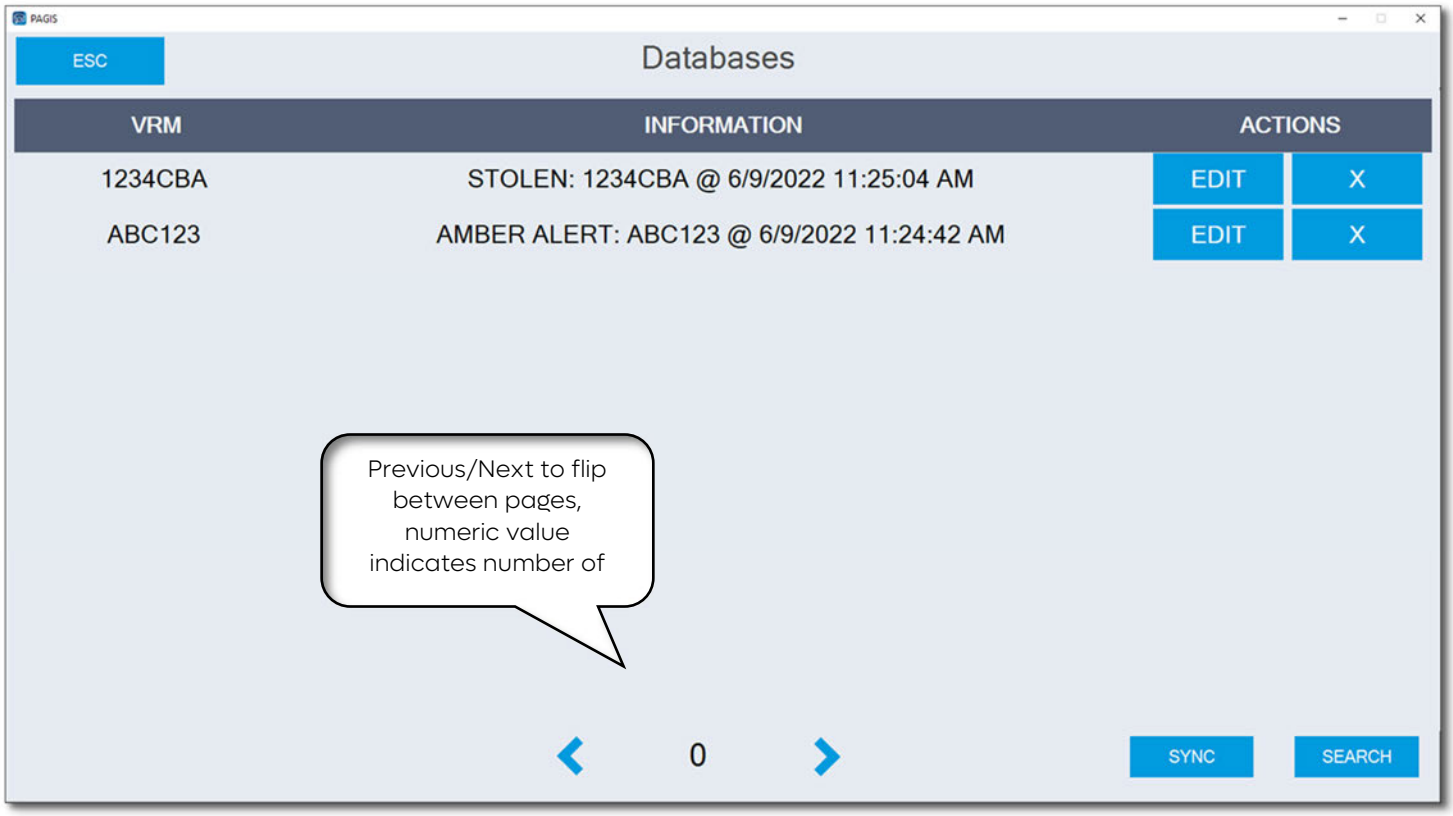
NOTE: Hotlist settings altered in PAGIS will be reset to their default configuration during the next Sync or End Shift. The default configurations are assigned by the BOSS Server/Administrator.

2976

2.14 Databases Edit- “Manual Reports”

Editing Hotlist has two function based on origin of hotlist.

- Hotlist deployed to PAGIS via BOSS cannot be edited, only the hotplates list can be viewed. Editing/updates are indented to be managed via BOSS.
- Hotlist created in PAGIS, i.e. “Manual Reports” can be managed by PAGIS users, allowing for changes or deletion of the hotplates contained within the hotlist.



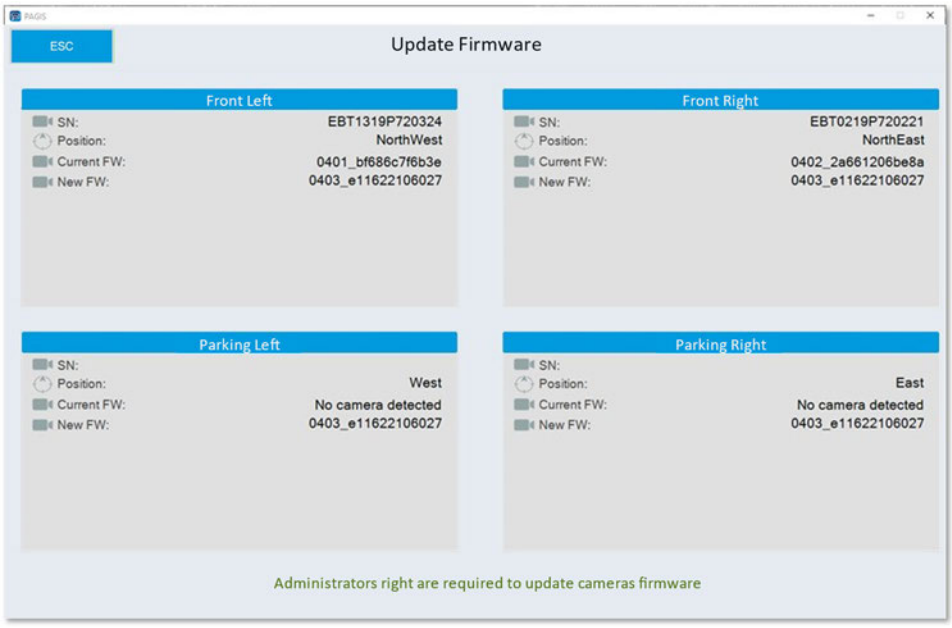
EDIT Button: Make changes to the indicustly hotplate information including licanse plate nuamber.
X Button: Remove indivualy hotlist from hotlist.
Previous/Next Button: Scroll thought lising of hotplates contaned within the hotlist. The numeric value indicates the number of pages.

2977

2.15 Software & Camera Firmware Update (Restricted Users)

Software and Camera firmware update provides a means for Neology to update the PAGIS and camera software to enhance and or correct performance. The Update icon will only apper when updates are avialable.

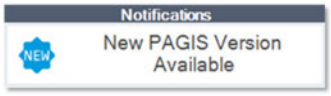
- The firmware update process only updates camera that are attached and function on the mobile processor.
- Restricted PAGIS users are only notified and displayed update information, only a PAGIS administrator can apply the FW update.



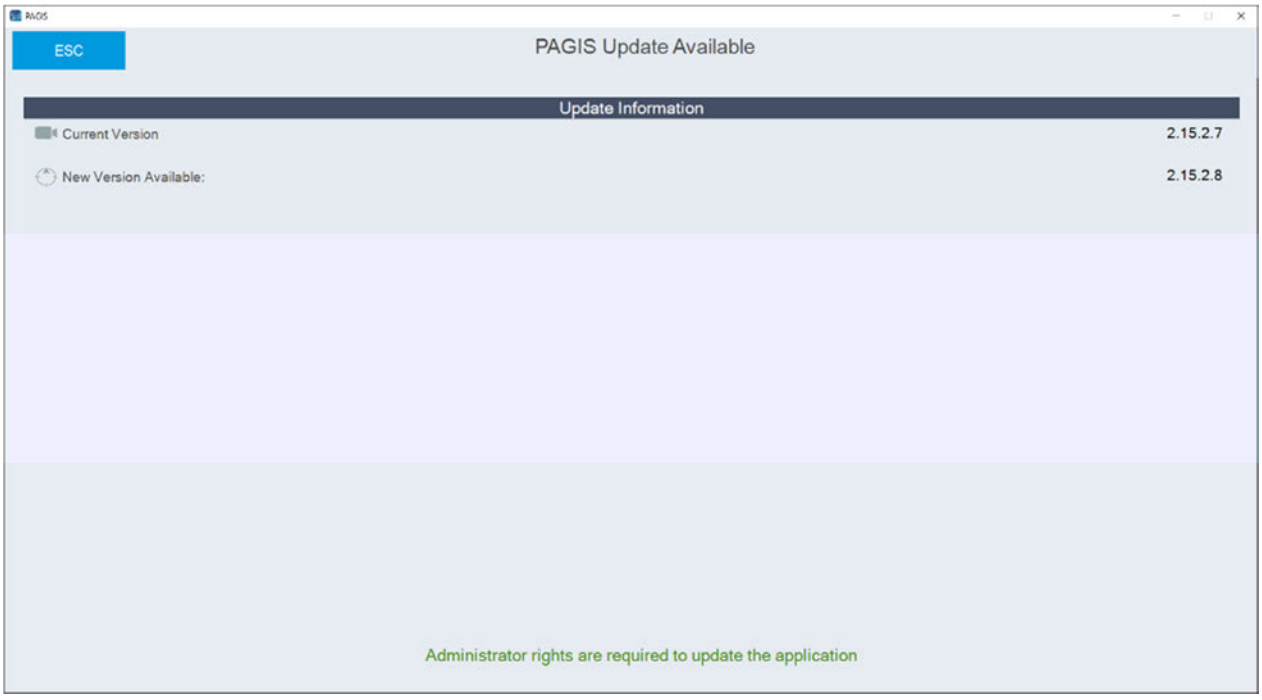
Firmware Updater Window List.

- Title “Camera Name”.
- Camera serial number.
- Position.
- Current FW version.
- New FW version available.

PAGIS Software Update



- When PAGIS update is available, you will see a notification banned.
- After clicking the notification banner, you will see the current PAGIS version and the newer version available.
- Administrator right are required to perform the update.



2978

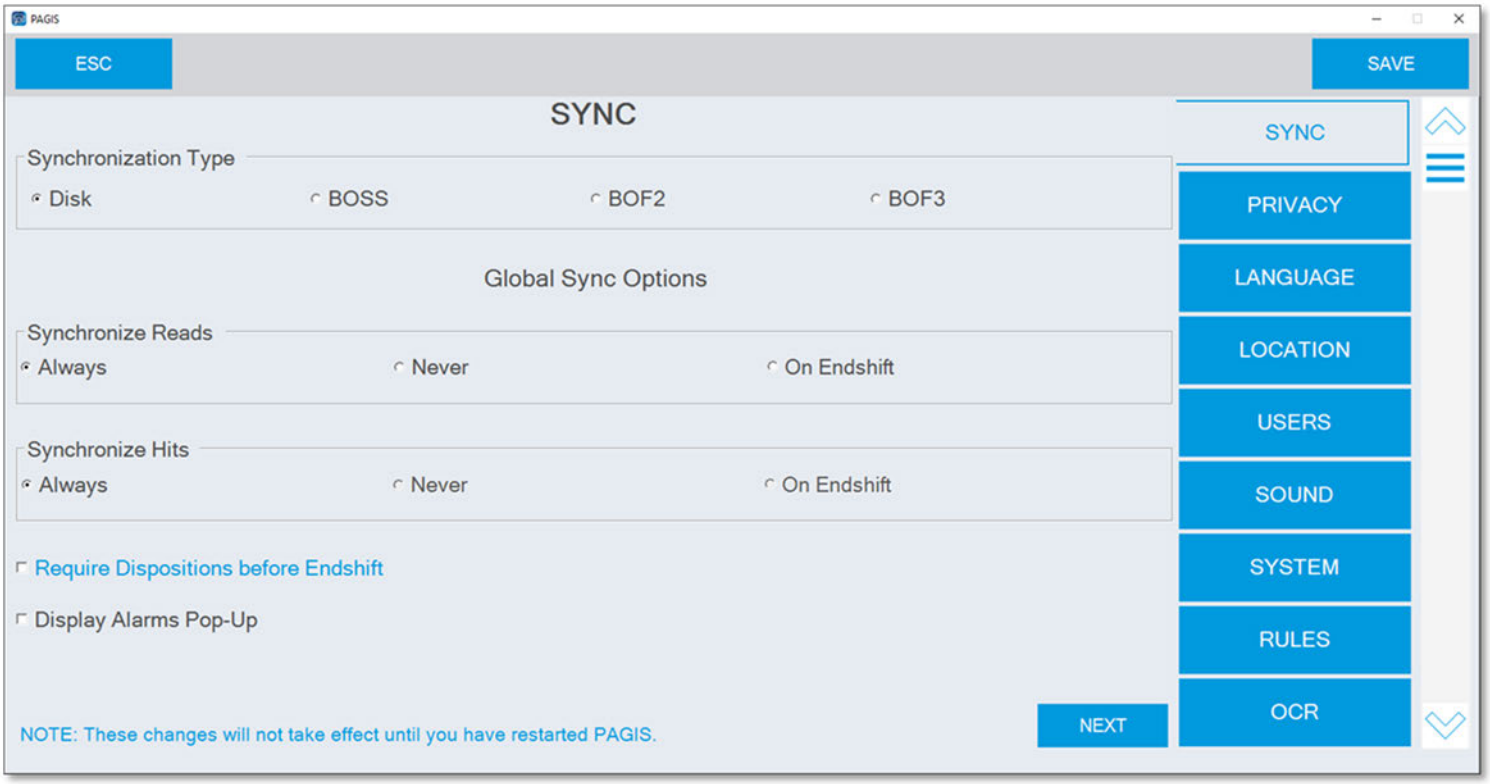
ADMIN SETTINGS

The Settings Menu is the central location for configuring PAGIS Software functions endpoint by endpoint. Users with Admin level rights in PAGIS can see and click on the Settings Button from the Live View Screen. Launching Settings opens the menu to the Sync Options Screen by default. NOTE: Users without Admin level access will not see this icon on the Live View Screen.

3.1 Sync Options Screen

As mentioned previously in sections 2.4 and 2.5, PAGIS uses various sync options to store, update, and synchronize ALPR data to and from the BOSS server. On the Sync Screen, Administrators configure the synchronization method and options.

NOTE: Configuration changes will not take effect until they are saved and the PAGIS Software has been restarted.



Synchronization Types

- **DISK**: Used to Sync standalone hotfiles directly into PAGIS or used to sync data with BOSS in offline mode.
- **BOSS:** Uses a wireless data network to Sync files to and from a BOSS server.
- **BOF2:** Used predominantly in Europe (see regional guide for support).
- **BOF3:** Used predominantly in Europe (see regional guide for support).

2979

Global Sync Options

Global Sync settings control how PAGIS synchronizes ALPR data during Begin and End Shift cycles and applies to both manually launched synchronizations as well as Auto-Sync functions. The two sections are Synchronize Reads and Synchronize Hits.



NOTE: All Hits are Reads, but not all Reads are Hits. A "hit" is a read that coincides with an Alert List. Due to this, the Options selected in the "Synchronize Reads" section dictate what options are available in the "Synchronize Hits" section. Unavailable options are greyed out.

- **Always:** Reads and Hits are synchronized to BOSS as close to real-time as the data network and PC processing allow.
- **Never:** The information gathered during the shift will be "sanitized" with each launch of End Shift. The corresponding data and images will NOT be sent to the BOSS server.
- **On End Shift:** Synchronization to BOSS will only occur when the user manually launches End Shift.
- **Require Dispositions before Endshift:** Requires the user to select a disposition code for each Hit registered in the PAGIS software since the last End Shift was completed before the Synchronization is processed.

3.1.1 Synchronization to Disk

Sync to Disk can support two distinct modes of operations. One mode is to only sync manual created hotlist into PAGIS using a defined set of rules, defined in Appendix B of this manual. The second mode is to manual synchronized data between PAGIS and BOSS when cellular or wireless data connection is not possible.

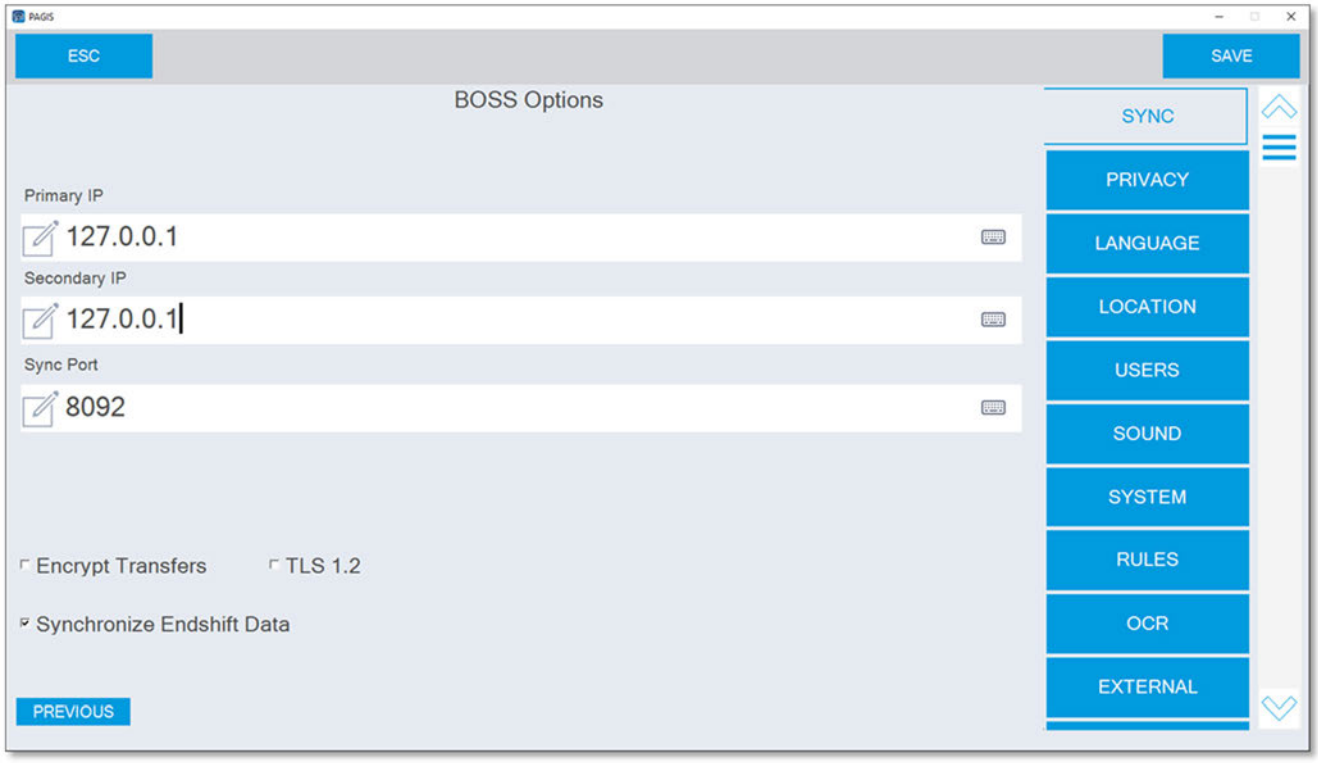


- **Drive Path:** In this text filed you must enter the correct drive path PAGIS will look for to sync data when using disk sync option. Do not include folder paths in this filed as PAGIS is expecting root patch for the Begin and EndShift folders.
- **Delete Beginshift Data on Sync:** The sync folder on the Flash Drive is deleted once all Begin Shift data has been imported to PAGIS. This is on by default to help prevent false alerts.
- **Encrypt Endshift Data:** All uploaded End Shift data created in PAGIS is encrypted. This is off by default.
- **Copy Endshift Data on Sync:** If unchecked, no End Shift data will be transferred to the Drive location.
- **Keep Only Updated Databases:** Removes any Hotlists from PAGIS that were not updated during Begin Shift as "outdated". This is off by default.
- **BOSS Files:** Must be enabled when syncing data with BOSS4 back office when using offline disk sync option.

2980

3.1.2 Synchronization with BOSS

Sync to BOSS is a streamlined method for updating ALPR data to the field units and the server. Additionally, selecting this option enables the PAGIS auto-sync features that synchronize data throughout the shift without user involvement.



BOSS Options Screen:

- **Primary IP:** The IP address of the BOSS server. This can also be the DNS name (NOTE: using DNS adds an additional failure point via the Domain Controllers and is not recommended as the best option).
- **Secondary IP:** Used for a secondary IP in cases where users switch from a cellular network to a Domain APN thus routing to BOSS from either an internal or external IP. This field can be left blank if not needed.
- **Encrypt Transfers:** When enabled, data transfers to BOSS will be encrypted.
- **Synchronize Endshift Data:** On by default, this enables PAGIS to sync to BOSS when End Shift is performed by the user.
- **TLS 1.2:** By default, PAGIS communicates using TLS 1.0 in its encryption layer, the TLS 1.2 option is provided as a mean for PAGIS to communicate on networks that are actively blocking the older TLS 1.0 & 1.1 protocols.

Sync to BOSS Prerequisites:

To establish the wireless sync to BOSS, the Agency Network Administrator will need to open TCP port 8092 to the BOSS server as well as define the internal and/or external IP address(es).

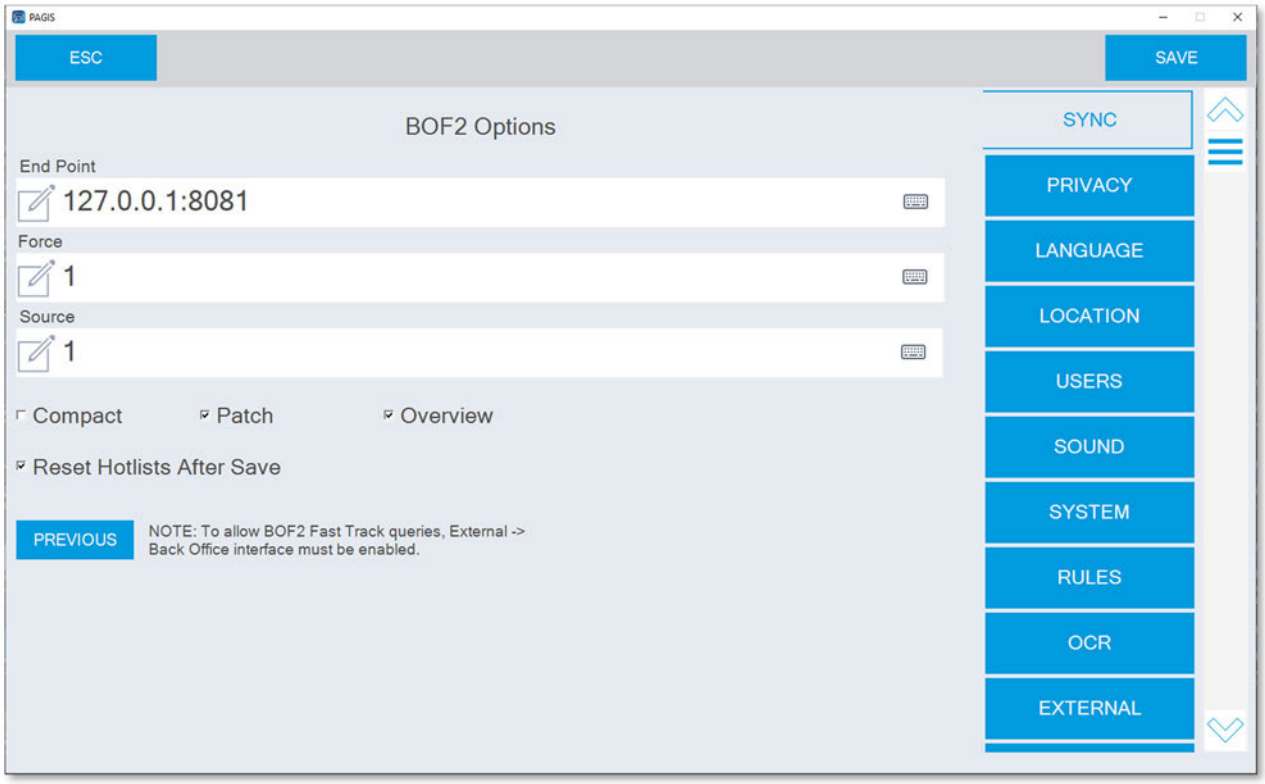
Sync to BOSS Setup:

From the Sync Settings Menu, the Admin must select the BOSS option and click the Next button. Then s/he will update the Primary and Secondary IP fields as necessary and de/select any options. Once configured, click Save to retain the changes. (For more information on PAGIS Auto-Sync settings, refer to section 2.4.3)

2981

3.1.3 Sync to "Instation" (Formerly BOF2 and BOF3)

The Instation software was formerly known as BOF2 & BOF3 and was developed by Anite PLC. It is a web-based Back Office software suite used in European markets to provide similar features as the BOSS server and UI Client.
NOTE: These options are NOT used in the Domestic United States.

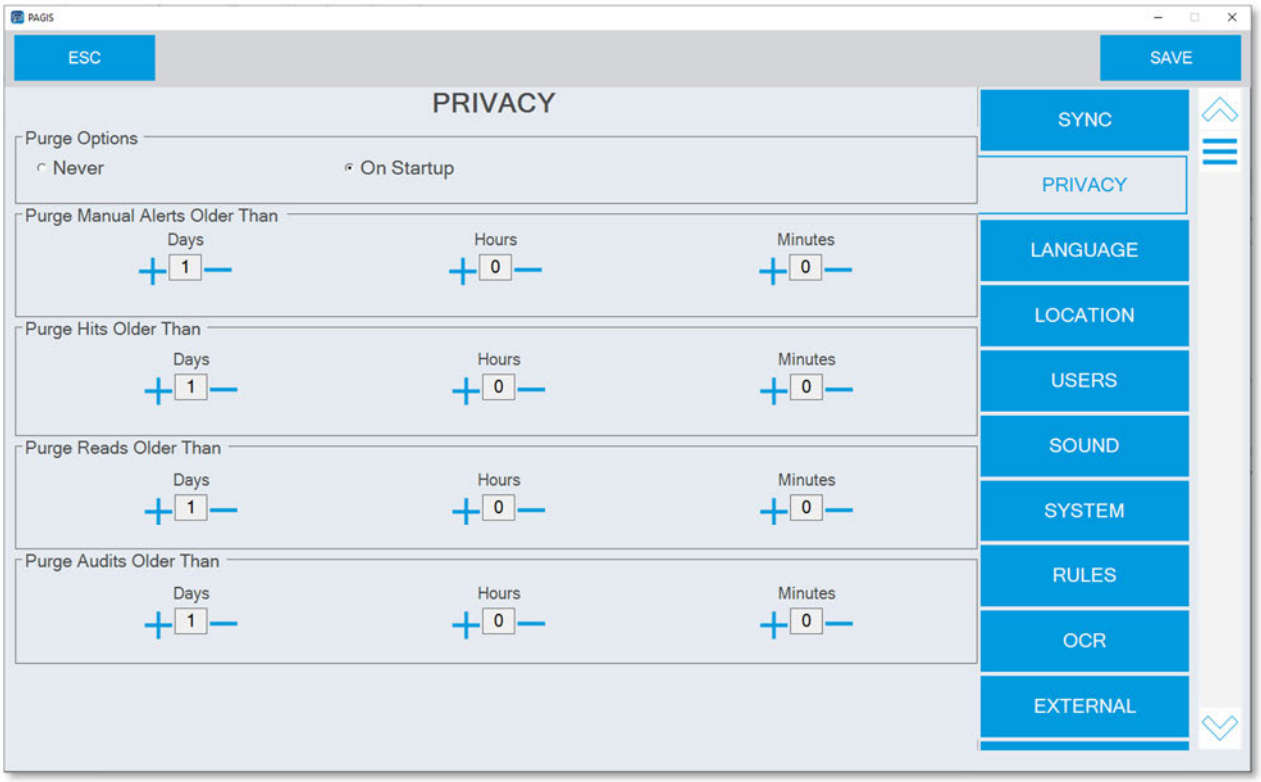


- **End Point:** The IP Address of the Instaion website. Format must be [IP Address:Port]
- **Force/Source:** Unique codes assigned to each police force.
- **Compact:** This option minimizes data transfer to Instation. Images will be deselected by default when in use.
- **Patch:** Refers to the image of the plate pulled from the read. This is on by default.
- **Overview:** Refers to the color overlay image from the read. This is on by default.
- **Reset Hotlists After Save:** When the software syncs to Instation, this will reset the hotlist tracking.

2982

3.2 PAGIS Privacy Settings (Local Data Retention)

PAGIS Software allows the Admin to configure the data retention settings for the local endpoint by minutes, hours, or days. This feature ensures the data captured/stored on the MDC is sanitized by the software itself (this is important for customers without BOSS). NOTE: To enable the Privacy settings, the Admin must select the "On Startup" purge option and then set at least one value in each row. Rows left with all Zero will not be sanitized or purged.



- **Never:** Selected by default, this option disables the PAGIS privacy settings and uses only those set in BOSS.
- **On Startup:** This option must be selected in order to enable the PAGIS privacy settings. Once enabled, PAGIS looks to purge/sanitize the system each time it's launched or restarted.
- **Purge Manual Alerts Older Than:** Controls how frequently all of the Databases/Hotlists in PAGIS are purged. The purge rate is calculated from the timestamp of the Hotlist. Once the retention value is surpassed, the Hotlist is deleted. Hotlists distributed from BOSS will be re-downloaded on the next Sync.
- **Purge Hits Older Than:** Controls how frequently all Hits in PAGIS are purged. The purge rate is calculated from the timestamp of the Hit. Once the retention value is surpassed, the Hit is removed the next time PAGIS is restarted.
- **Purge Reads Older Than:** Controls how frequently all Reads in PAGIS are purged. The purge rate is calculated from the timestamp of read. Once the retention value is surpassed, the Read is removed the next time PAGIS is restarted.
- **Purge Audits Older Than:** Controls how frequently all Audits in PAGIS are purged. The purge rate is calculated from the timestamp of the audit. Once the retention value is surpassed, the audit is removed the next time PAGIS is restarted.

NOTE: Once Reads, Hits, Hostlist or Audits have been purged, they can no loner be viewed in the PAGIS software.

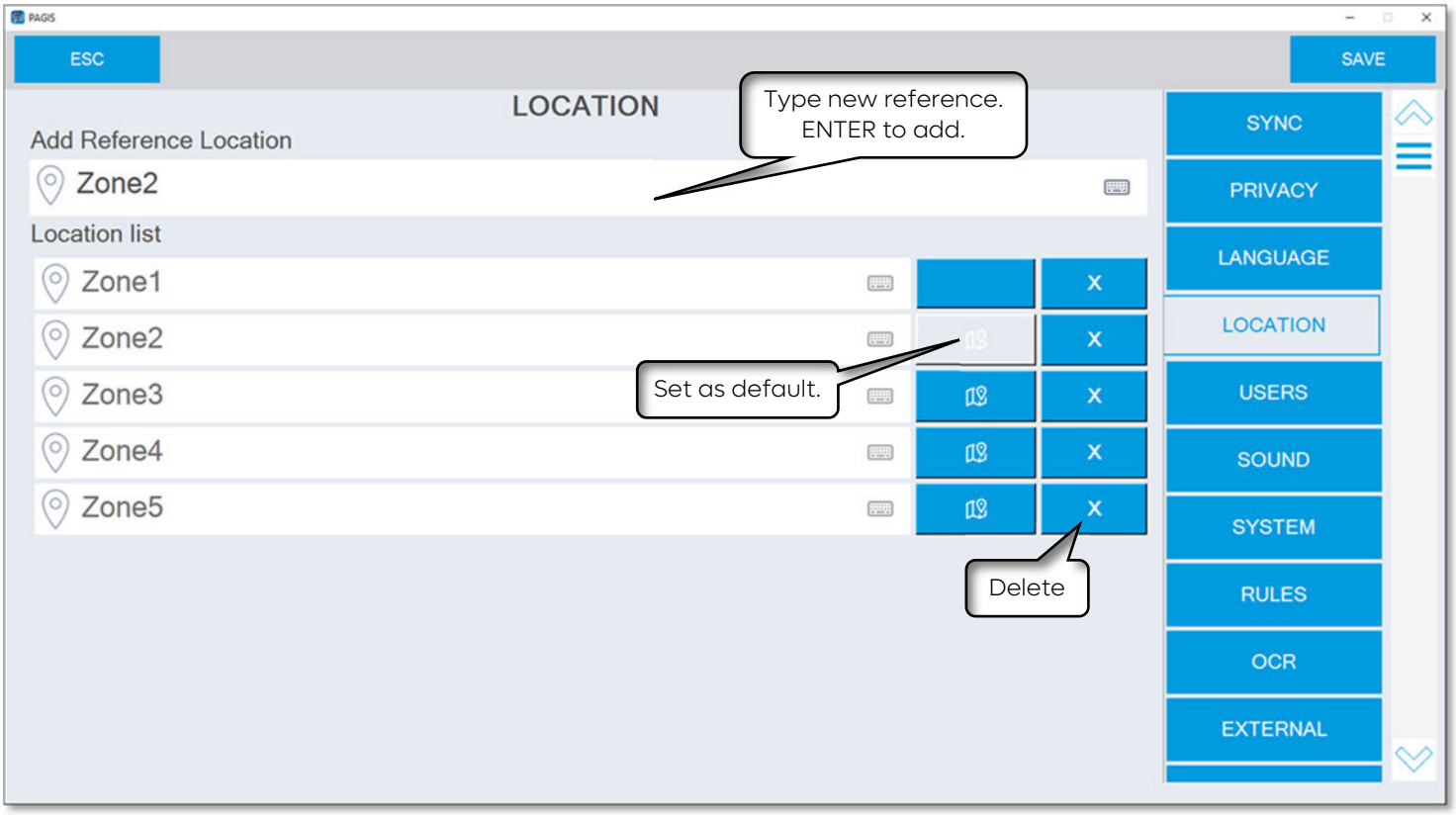
2983

3.3 Language

The Language screen allows the Admin to change the language assignment used in the PAGIS Software. Available languages are listed in the drop-down list and are added during the installation process.

3.4 Location

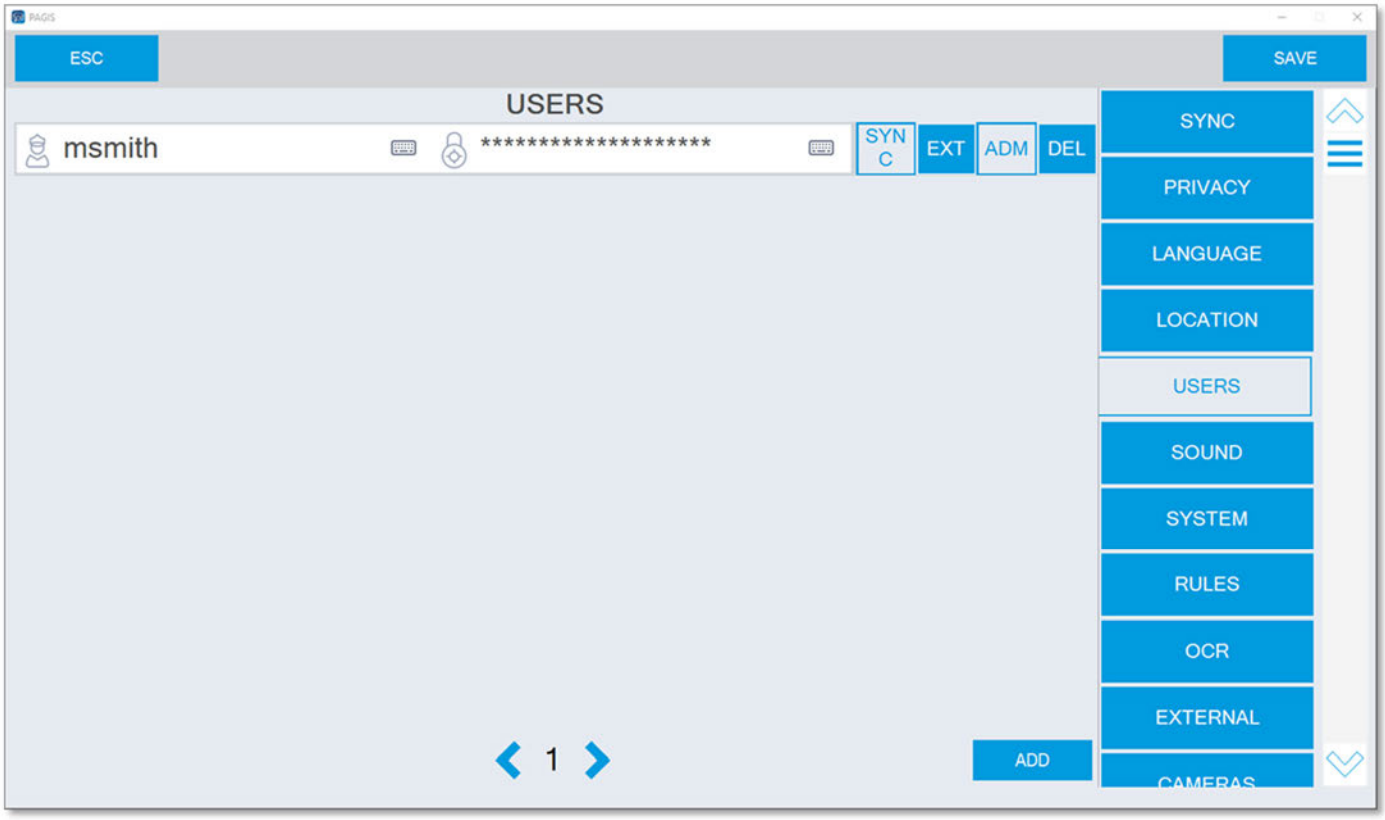
Updates to the location field will auto-fill the "Reference" section of the PAGIS Login Screen. These are often used to specify a patrol region (Examples: "North Patrol" or "A2"). Once designated all reads/hits will show this designation. Muiltiple "Referance" location can be added, the available list can then be selected from the login screen.



2984

3.5 Users

User accounts, credentials, and rights are generally administered from BOSS and then distributed to the PAGIS via the syncrniztion process. However, PAGIS does allow for Administrators to add and delete users as well as set their privileges directly from PAGIS.



NOTE: Adding user directly in PAGIS should be limited to customers not utilizing a BOSS server. User accounts created directly in PAGIS by customers with BOSS will be overwritten/removed during the next sync.

Adding a User in PAGIS:

1. From the Settings Screen, select the USERS Button on the Right.
2. Click the ADD Button.
3. Enter the case sensitive username in the Username Field (max of 15 alphanumeric characters).
4. Enter the case sensitive password in the Password Field (max of 15 alphanumeric characters).
5. Select the User's privileges
6. Click the SAVE Button to apply the changes.

User Privileges

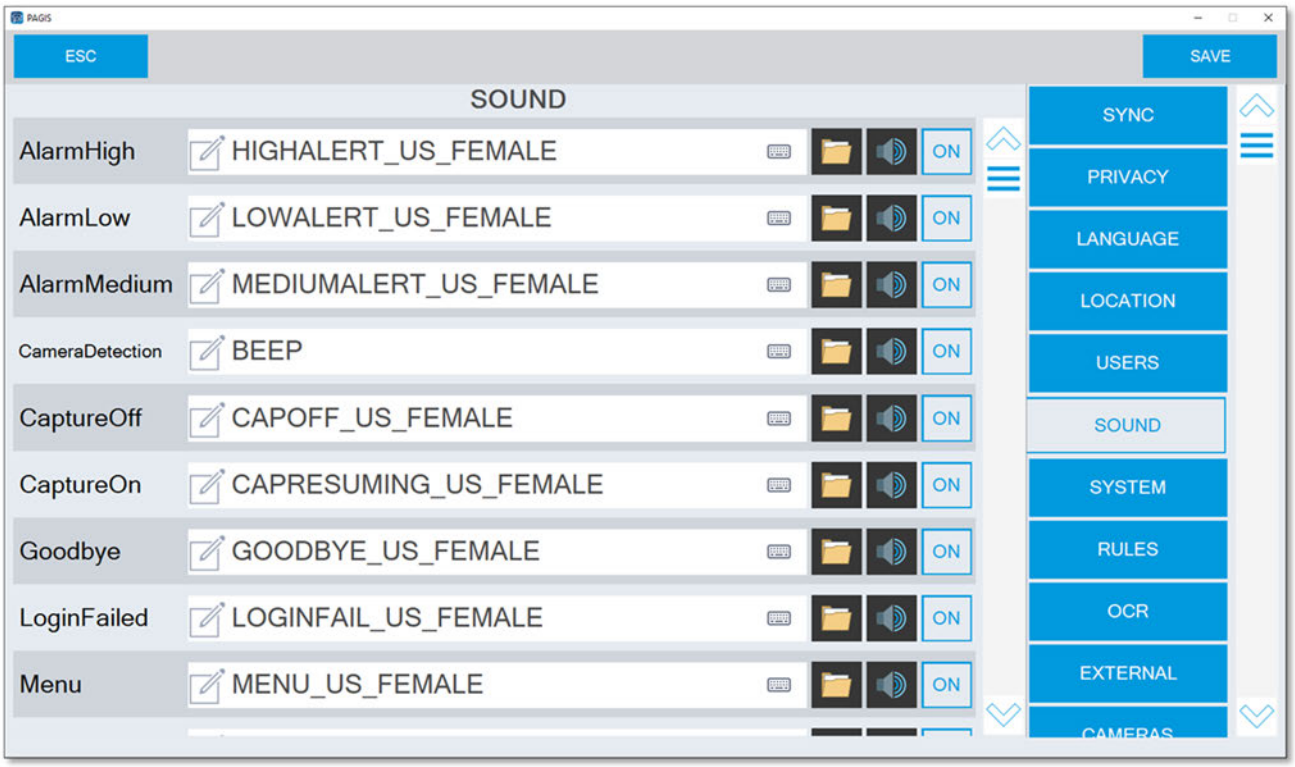
SYNC: Allows users to manualy synchronize data.
EXT: Allows the user to import external Hotlist from disk sources..
ADM: Provides the user Admin rights and allows him/her to configure the PAGIS Software.
DEL: Allows the Admin to delete a User from the list. Click once to select and the save button to delete.

NOTE: Creating a new user in PAGIS automatically deactivates the default user account settings (Section 2.1.1).

2985

3.6 Sound

Sounds in PAGIS mirror the user or software activity (Ex. Login, Audible alert from a "Hit", and Logout) and are On by default. PAGIS Administrators can adjust the sounds from the available presets and/or load unique .wav files onto each PAGIS for custom sounds. **NOTE:** The default storage path is "C:\Program Files\PlateReader\MDC\sounds".



Configuration Buttons

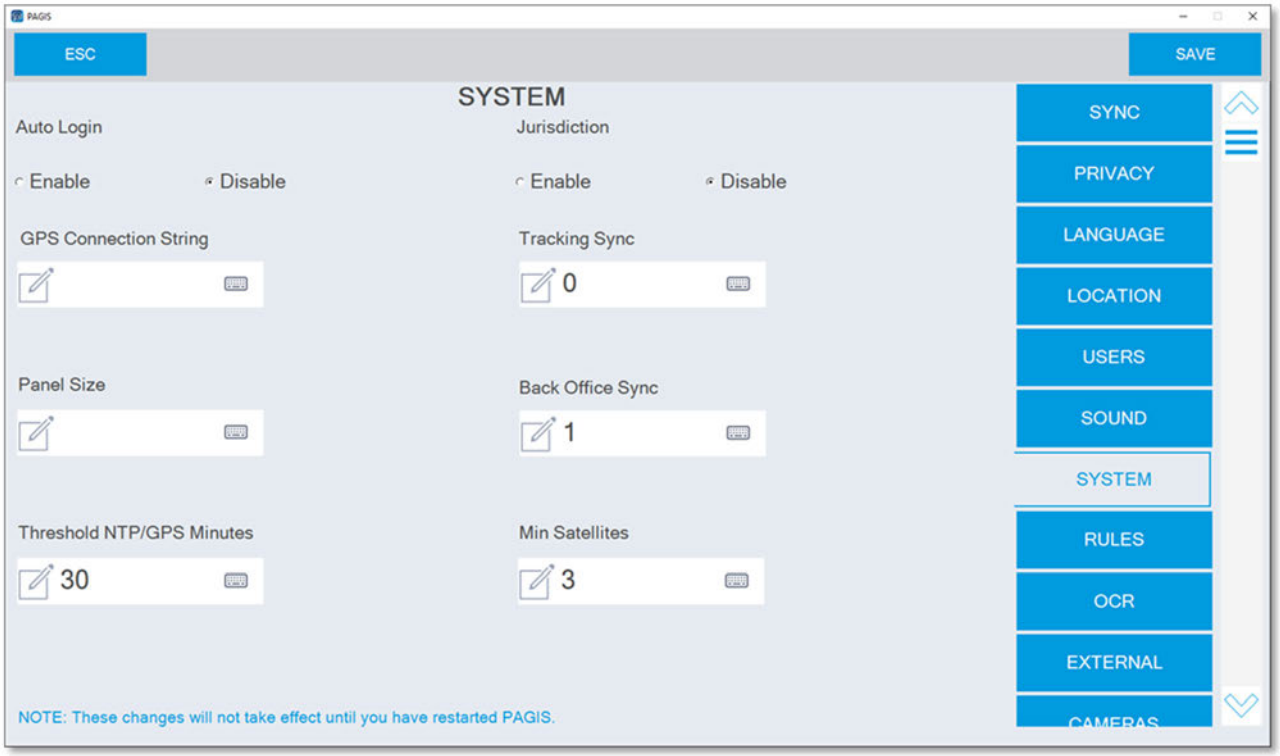
The sounds listed on the configuration screen can be altered or updated by PAGIS administrators using the buttons below. **NOTE:** Changes to any sounds must be saved before they can be played in PAGIS.

	Click to browse to the sounds folder. This is used to select a new sound file.
	Click to Test/Play the selected sound.
	Shows the status of that sound. Click to turn each sound Off.
	Shows the status of that sound. Click to turn each sound On.

2986

3.7 System

The System screen determines external system connections, Login behaviour, Panel size.



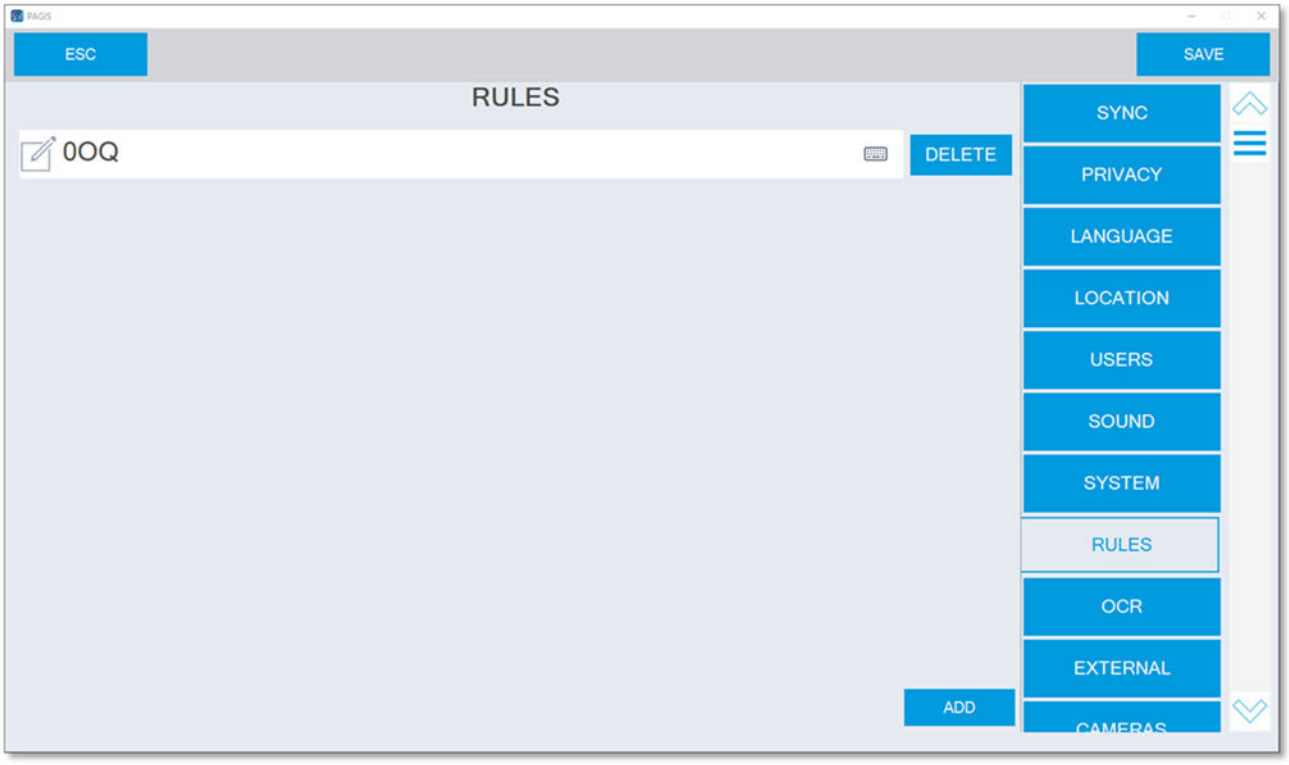
- **Auto Login:** Enabling this feature will disable the login screen and login to PAGIS as the Admin automaticaly. This feature is recommended only for unattended use Speed-Trailer applications and Covert Drop and Go deployments. **Note:** If PAGIS login accounts are deployed to PAGIS, it will disable the auto login feature.
- **GPS Connection String:** The GPS string is utilized to redirect PAGIS to acquire GPS feed from different source. Defaults for client PAGIS (MDC) is no value and 6 for Standalone. The GPS connection string defaults to a COM port value, although it may also refer to TCP/IP: Port option if IP is included in the connection string, example (127.0.0.1:8080).
- **Panel Size:** Controls the resolution of the color image displayed on the Live View Screen. By default this is blank as PAGIS controls the aspect ratio. However a PAGIS Admin can assign custom resolutions in WxL format (720x1024) to assist with non-standard dispalys.
- **Threshold NTP/GPS Minutes:** This setting controls the behavior of the GPS lock status. If the threshold value (which is obtained by calculating the difference between the time of the last packet received from GPS and the current time) is greater than the value configured in minutes, then GPS status will change to Not Locked indicating it did not receive an updated GPS signal.
- **Jurisdiction:** This feature enables State recognition of the captured plate origin. Note- *This is a BATA feature and Neology makes no claims on its performance capabilities.*
- **Tracking Sync:** Controls the sync intervals in (Sec.) that PAGIS communicates with BOSS4 to update tracking status. Default off=Zero, values can range from 1-9999. BOSS4 Back Office Software requiered for this feature.
- **Back Office Sync:** This setting controls the sync timing that PAGIS sends data back to BOSS3/BOSS4, Timing is in (Sec.), default is 10sec, values can range from 0-9999.
- **Min Satellites:** This setting controls the behavior of the GPS lock status if the minimum number of Satellites set is not met, when value is not met the GPS status will change to Not Locked.

NOTE: All changes must be saved and will not take effect until PAGIS is restarted.

2987

3.8 Rules

Rules provide a way to check for commonly misread character by creating a set of rules for checking against available Hotlist. For instance, "8" and "B" are sometimes mistaken. If the OCR engine reports a plate as ABC123, you might want PAGIS to check both ABC123 and A8C123 against all Hotlist to find a match. While PAGIS is less likely to miss a Hit, the process can also produce more false Hits.



Adding a Rule to PAGIS:

1. Click the ADD Button.
2. Enter the desired alphanumeric characters (Ex. 0 and O) into the text field.
3. Click the Save Button at the top right of the screen to confrim the rule.

Deleting a Rule:

1. Locate the rule to be removed from PAGIS.
2. Click the DELETE Button to the right of the rule.
3. Click the Save Button to complete the removal.

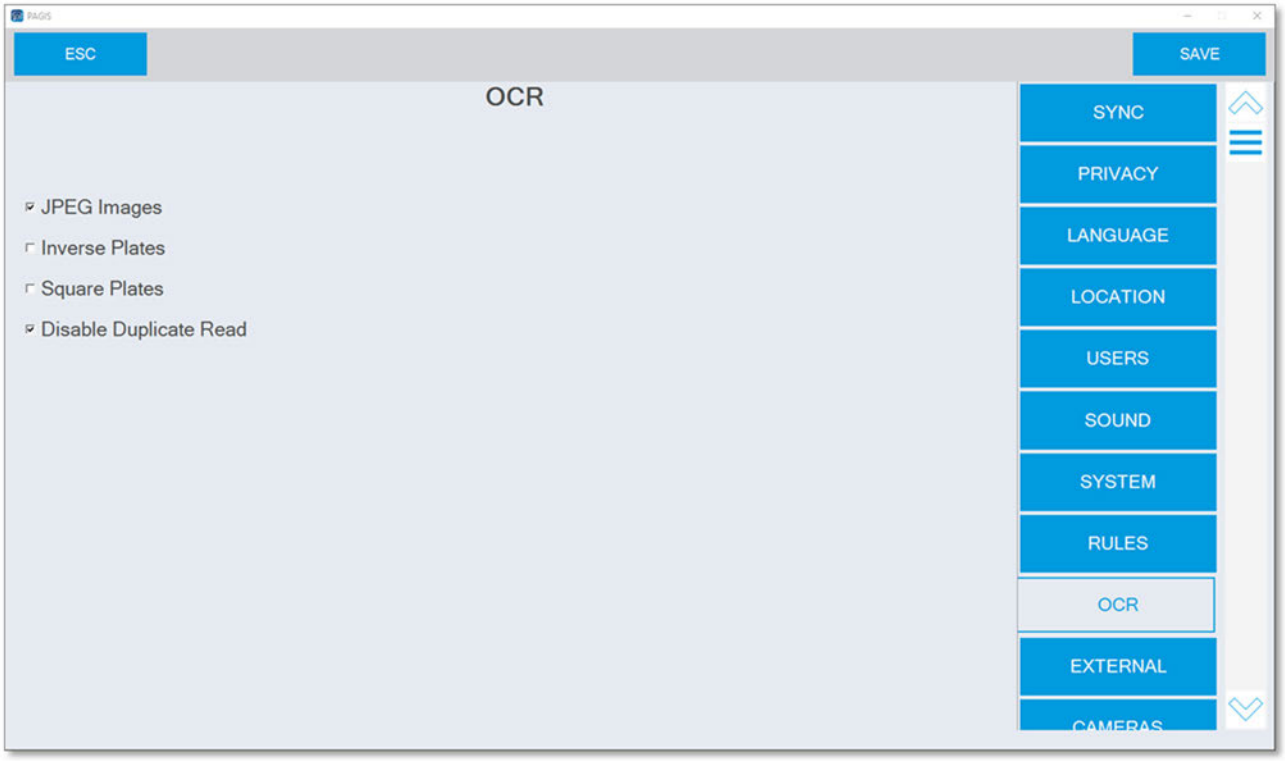
Rules – Additional Clarifications

1. Rules are processed based on the first character entered. So in order to read any O as a zero, the Admin will need to add rule "O0". And in order to read any zero as an O, a second rule must be entered as "0O".
2. Rules are NOT designed to overhaul OCR function. Any consistently misread values should first be brought the attention of Neology Support for review. And only those cases where further adjustments to the OCR software are impossible would rules be recommended.
3. Adding rules to PAGIS will make it less likely to miss a Hit Alert. However, it will increase the number of Hit Notifications that require the Officer to visually confirm the OCR read ("IR Patch") and the Hotlist Alert match.

2988

3.9 OCR

The OCR Section in PAGIS provides Administrators some additional options on how they would like PAGIS to process plate reads.



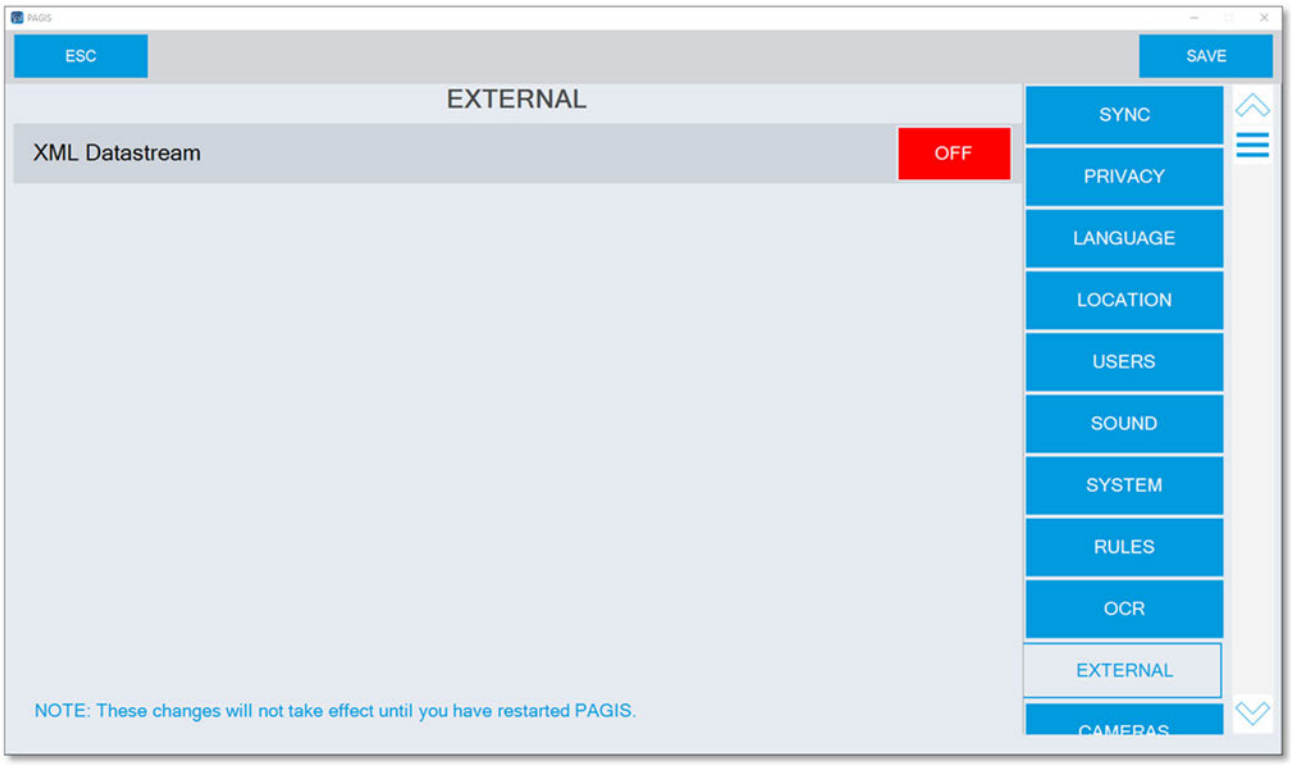
- **JPEG Images:** On by default, this forces PAGIS to use compressed .JPG images instead of the full resolution Bitmap images each time a read is taken. This settings minimizes data storage requirements and preserves disk drive space.
- **Inverse Plates:** Off by default, this setting is only used in States where plates with light color lettering over a dark background are prevalent. Enabling this option increases processing load and should remian disabled unless required.
- **Square Plates:** Off by default, this setting adjusts the read area plates that are square instead of retangular.
- **Disable Duplicate Read:** On by default, this setting helps PAGIS prevent duplicate plate reads. If a VLP is read by more than one camera within a short period, the duplicate read is ignored. This minimizes data storage requirements and improves overall system metrics related to numbers of Hits and Reads.

NOTE: Once changes are made, the Admin must click the Save Button in the upper right corner to retain them.

2989

3.10 External

The External Screen allows the Admin to connect PAGIS to an external database or device via XML Datastream. This feature is Off by default and any changes must be saved before they will be available.



Enabling the Datastream:

1. Click the OFF Button to toggle to ON.
2. Click the Save button in the upper right corner to apply.
3. Restart PAGIS.

NOTE: Enabling this feature will reduce the overall performance of the PAGIS Software.

XML Datastream Ports

The connection to the datastream is via TCP/IP ports. Metadata is passed in real time and images are pushed periodically.

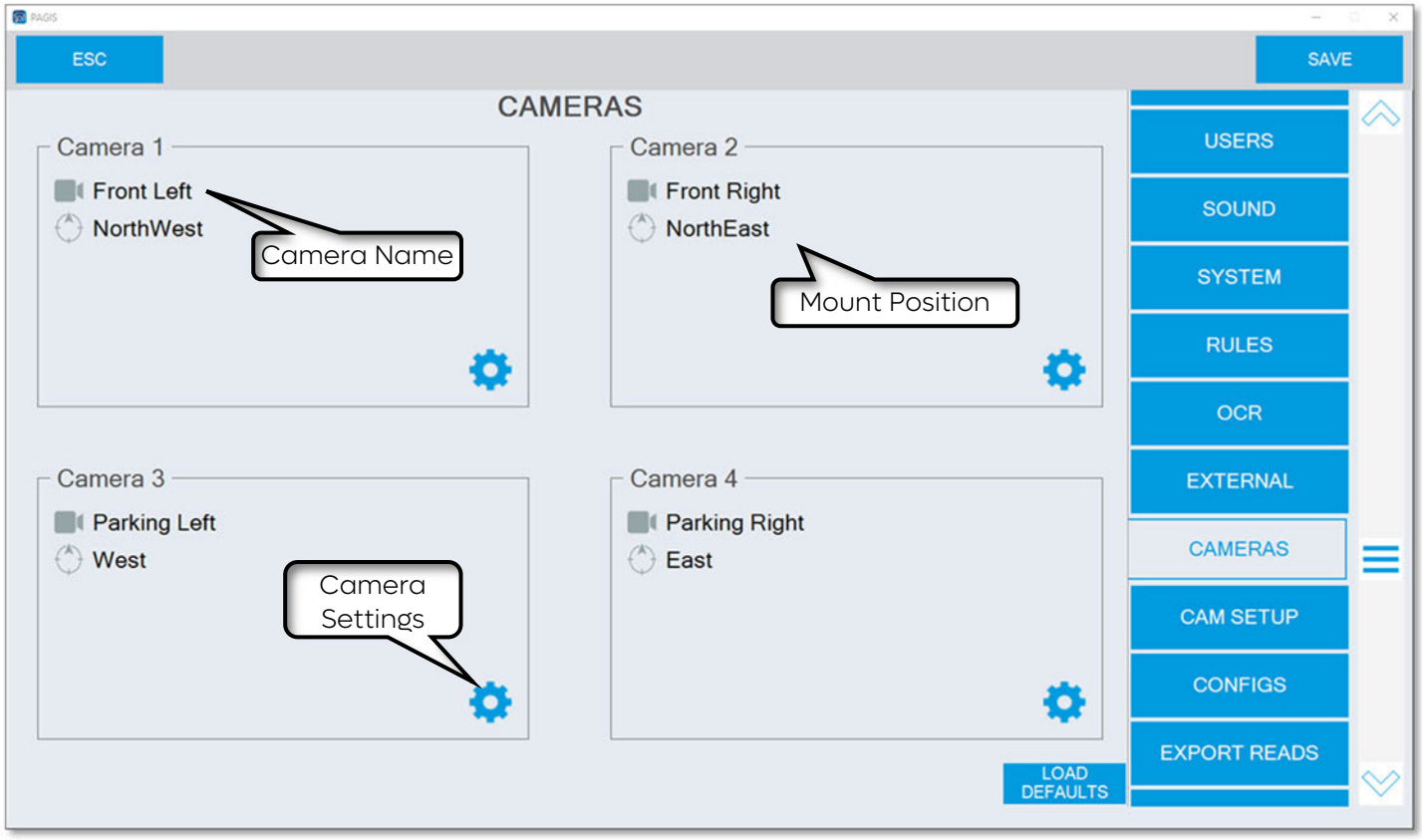
1. Query Port: TCP 7000
2. XML Datastream/Heartbeat: TCP 10100

NOTE: Greater detail on the XML Datastream can be found in Appendix D

2990

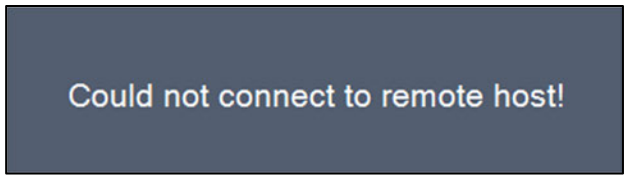
3.11 Cameras

The Camera setting panels are a software representation of the physical camera ports located on the mobile processor. Each camera panel has its own unique settings that can be altered to accommodate custom application.



Camera Connection

In order to configure the cameras, the PAGIS Software and the Processor must be able to communicate. If they cannot, the Administrator will receive the error message below as soon as he or she clicks on the CAMERA Button indicating that PAGIS cannot "see" the cameras. See Appendix C FAQ for troublshooting tips.



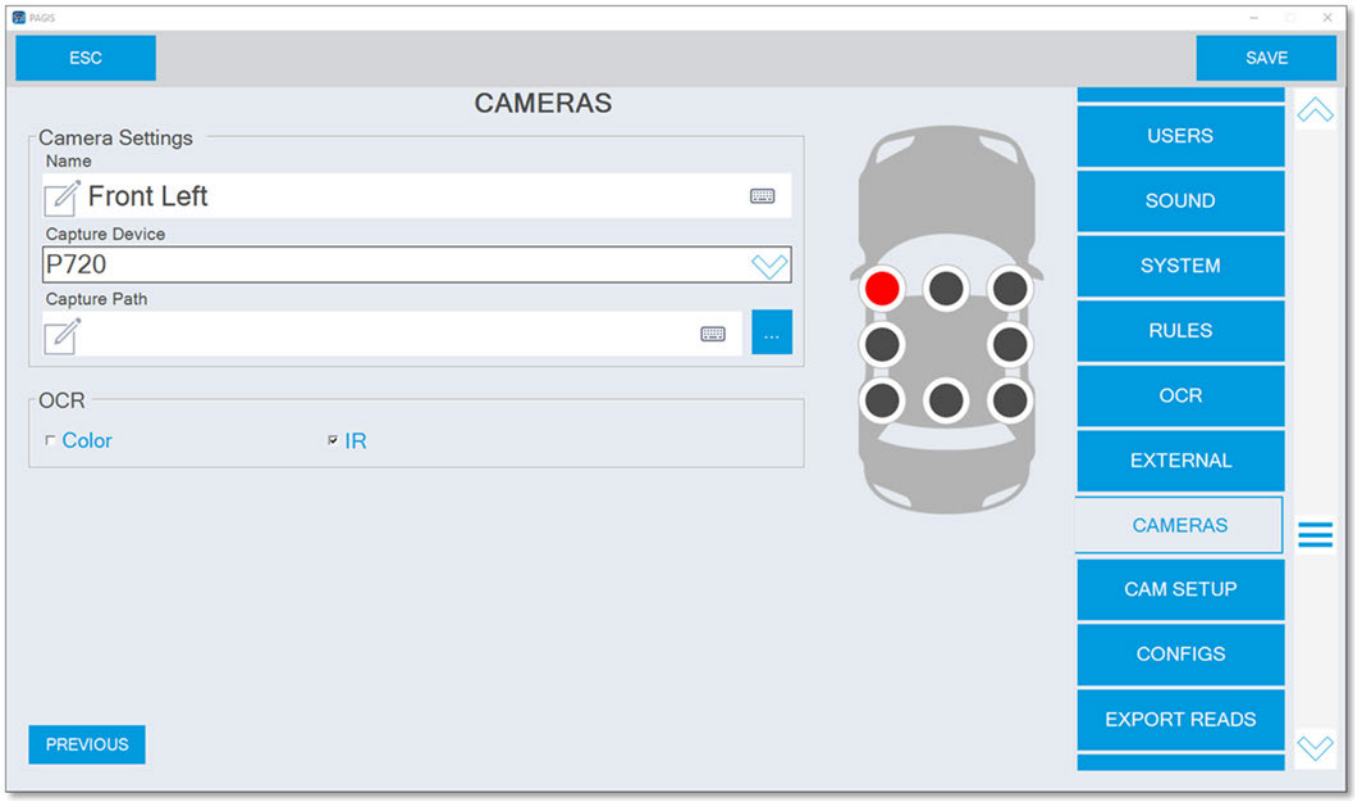
2991

3.12 Cameras Settings

This section will assist with the general configuration of the cameras. Administrators can begin by selecting the Settings Icon to edit each of the existing cameras or by selecting the Load Defaults Button.

Camera Settings (Edit) Screen

This provides the Admin a single screen to edit the name, confirm the capture device, assign camera position, and confirm OCR settings.



- **Name:** The Camera Name field accepts 50 characters, but PAGIS will only display 11 characters on the Main View screen.
- **Capture Device:** The connected mobile processor delivers the device type to PAGIS when entering the "Camera" settings section, options are P720 for SX4e and P442 for SX4 models. Other options are video files, user feed and client for development use only.
- **Capture Path:** Configure PAGIS to aspect IP based video feeds and .AVI video file paths, for development use only.
- **OCR:** Activate OCR for Color or IR cameras or both.
- **Camera Position:** This Symbol indicator is for the alert screen to indicated camera placement direction.
- Click the Save Button to retain the changes.

Cameras Settings (Load Defaults):

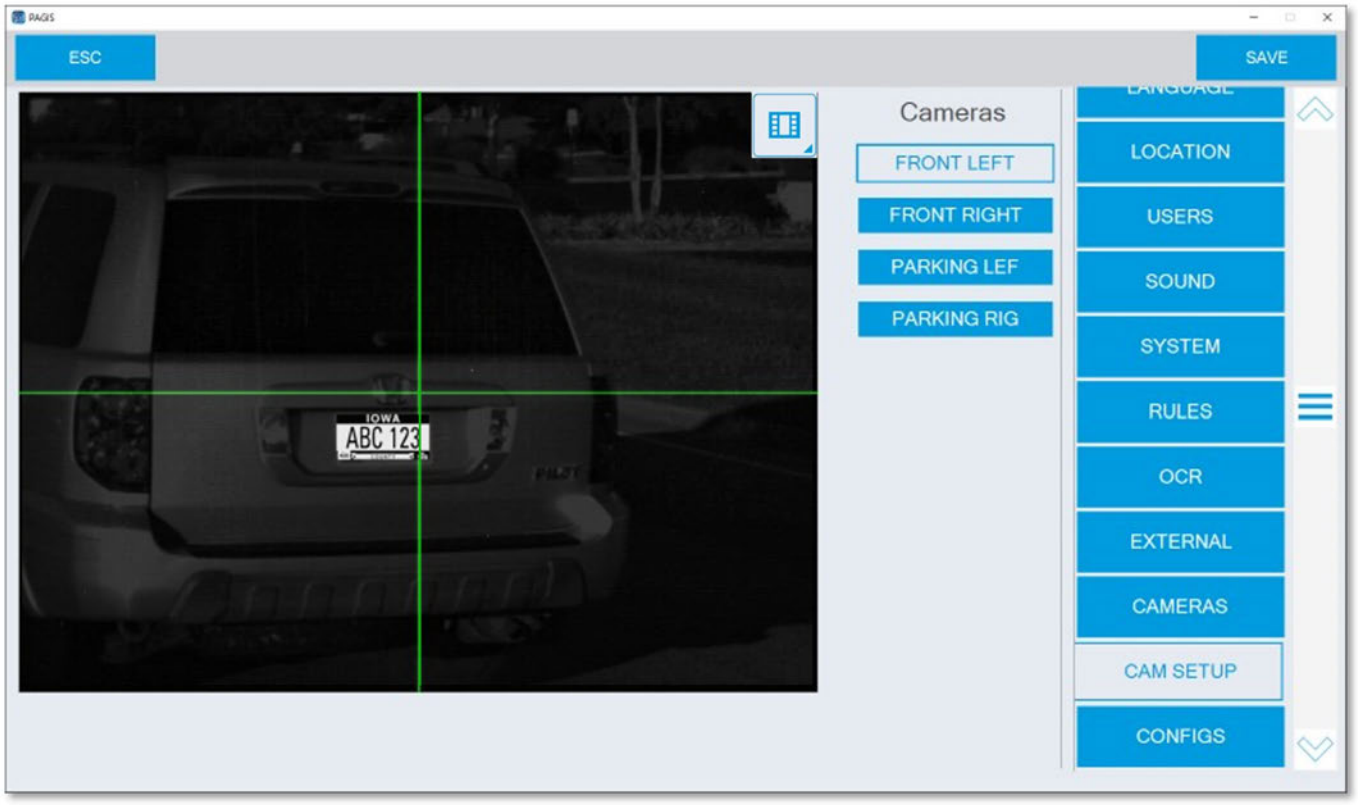
Load defualt camera setting will overwrite any existing cameras and config setting to thiere factory defualt vaules.

1. Click the LOAD DEFAULT Button in the lower right portion of the Cameras Screen.
2. Locate "Default" and click the LOAD Button.
3. Click Save to apply, (This returns the Admin to the Cameras Screen).
4. Click the Camera Settings Icon to inspect and configure each camera one at a time if needed.

2992

3.13 Cam Setup

The Cam Setup Screen presents Administrators with a live preview of the configured cameras. This section also allows the Admin to switch view modes from Color to IR to ensure the system is functioning properly. This screen can also be utilized as a means to align newly mounted cameras.



Cam Setup Navigation Buttons

The Admin may view the output of each camera by clicking on the camera name. When a camera is selected, the button will turn grey to indicate it has been selected. In order to switch view modes, the Admin must use the following buttons:

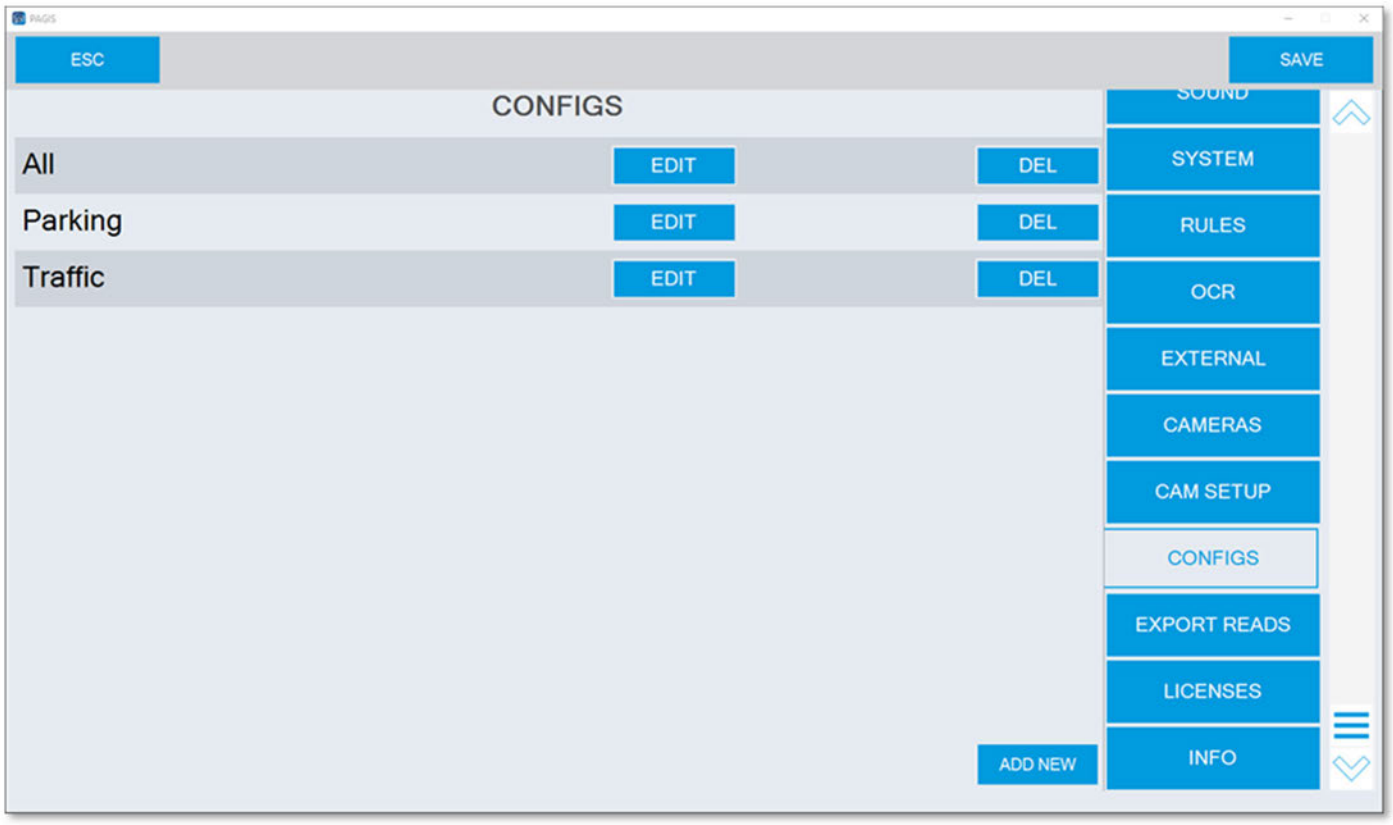
	**Color View:** The Color View Mode is the default view when entering Cam Setup. This displays a live preview of the color camera video feed
	**IR View:** By clicking on the Camera View Selector button, this will switch to the Infrared (IR) View Mode. This displays a live preview of the IR camera video feed.

NOTE: Unlike the main Live View Screen, the camera feed shown on the Cam Setup page will not time out when in use. This feature makes it easier for the Administrator to review and align the mobile cameras.

2993

3.14 Configs (Camera View Modes)

The Configs Screen allows the Admin to construct how the cameras will be displayed on the Live View Screen for the user. This section also allows agencies to create multiple viewing configurations to meet specific environmental needs or to add greater functionality to the software. By default, the Configs layout provides the agency with three camera modes, "ALL", "Traffic" and "Parking". All mode dipalys the front two cameras and rear two are activated, Traffic mode only displays the front two cameras and rear cameras are off, Parking mode only displays rear two cameras and front cameras are off.



Configs Navigation Buttons

To properly configure the camera modes used in PAGIS, the Admin will navigate this section with the following.

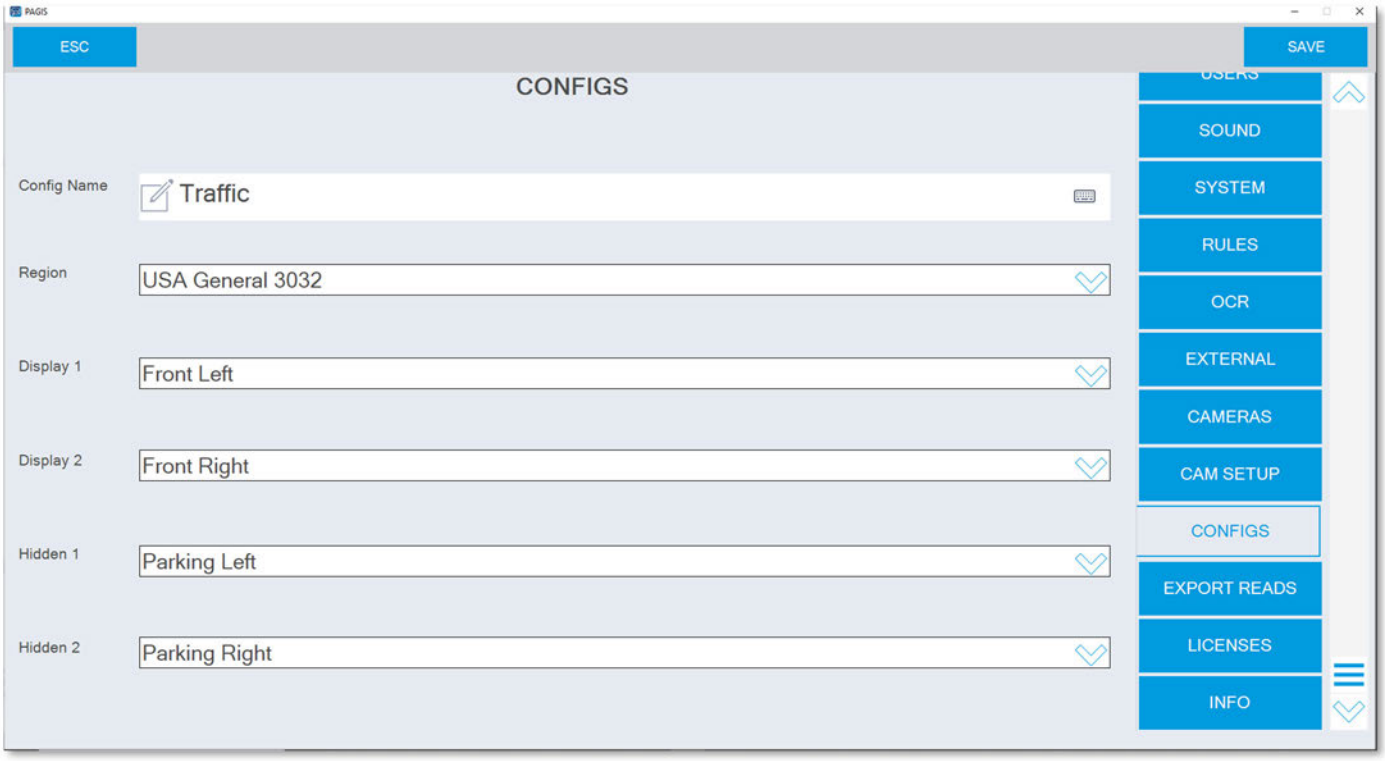
- EDIT: Modify the mode settings for the selected configuration, including selecting a region OCR and selecting which cameras are displayed or hidden.
- DEL: Removes the current configuration from PAGIS.
- ADD NEW: Creates a new config mode.

NOTE: The number of Configs equals the number of Camera Modes available to the user from the Live View Screen. Each camera mode untilizes the Config name established in this section. Users cycle through the modes on the Live View Screen by clicking the Mode Selection Button in the upper left corner.

2994

3.15 Config Settings

When getting started, most Administrators will begin by simply modifying the existing camera modes or "configs". The following example will demonstrate the standard configuration of a four-camera mobile unit.



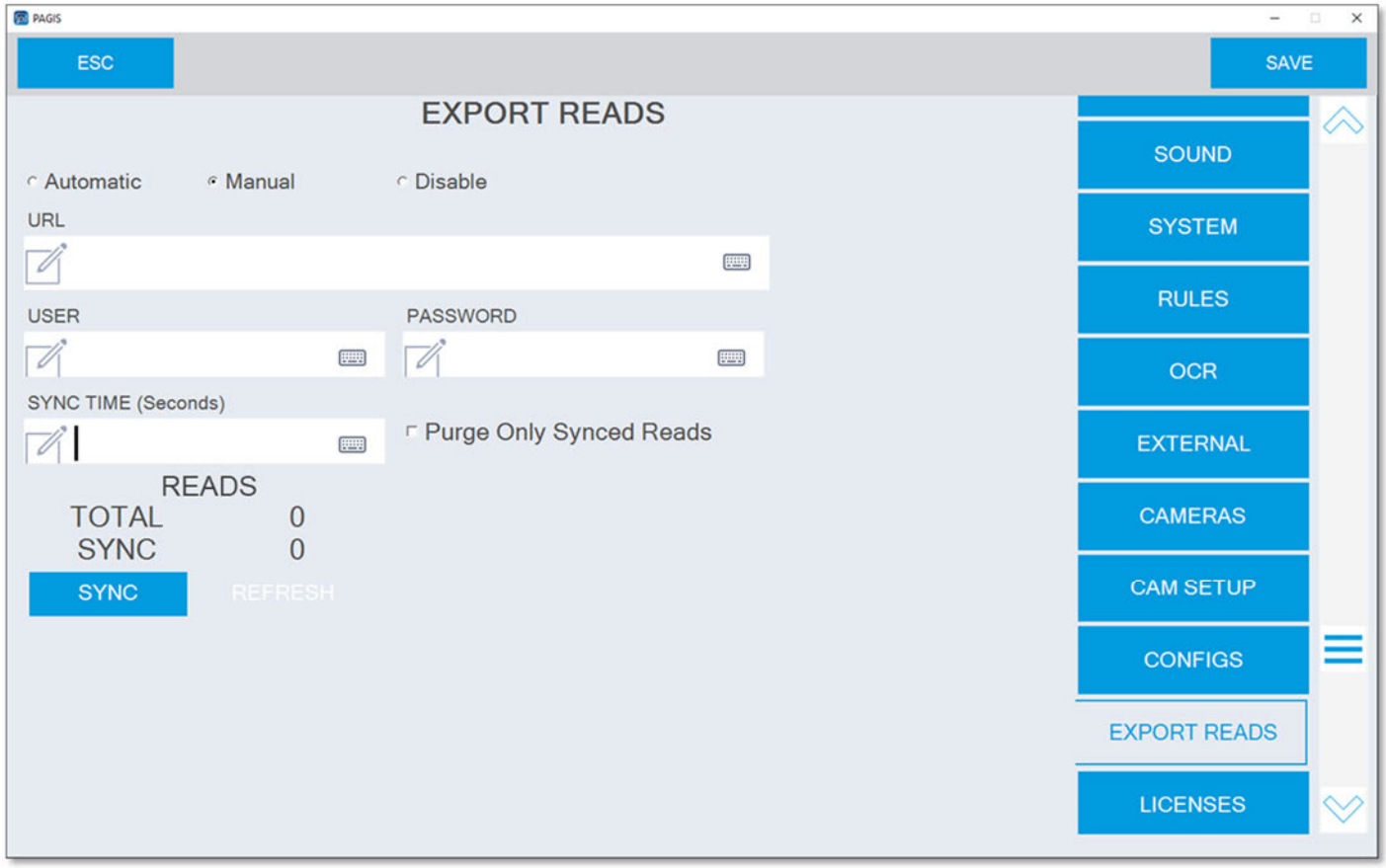
- **Config Name:** The name of the configuration mode.
- **Region:** Select region file to be used, these are preloaded at the time of purchase. This setting must be applied on first setup or cameras will not capture plates.
- **Display 1:** This camera is always displayed on the left-hand side of the Main View screen.
- **Display 2:** This camera is always displayed on the right-hand side of the Main View screen.
- **Hidden 1 and 2:** When populated, these cameras are functioning and performing OCR, but the images are not visible to the user. Hits and Reads will still be generated by these cameras and alert still notify users.

NOTE: In situation were the cameras need to be temporarily turned off, you can create a mode called GoDark, select region but do not select any cameras. Once this mode is select in PAGIS the cameras will go into standby, turning off the cameras LED's.

2995

3.16 Export Reads

The PAGIS data export feature allows for the ability to export data to a RestAPI service for distrabution redirect. This feature is licensed and will not display in the PAGIS menu until the licensing is applied.



Feature Requirement:

- Must obtain License file to enable this feature.
- Must place license file into Licenses folder where PAGIS is installed, typically "C:\Program Files\PlateReader\MDC\Licenses".
- Must have a working RestAPI service ready to except posted data from this feature. The Export Reads feature is a POST method only.

Set Sync Behavior:

I. **Automatic:** Set data to sync automatically in specified time intervals. REFRESH button will update the READS status indicator.
II. **Manual:** Set data to sync manually using the SYNC button.
III. **Disable:** Disable export.

Feature Settings:

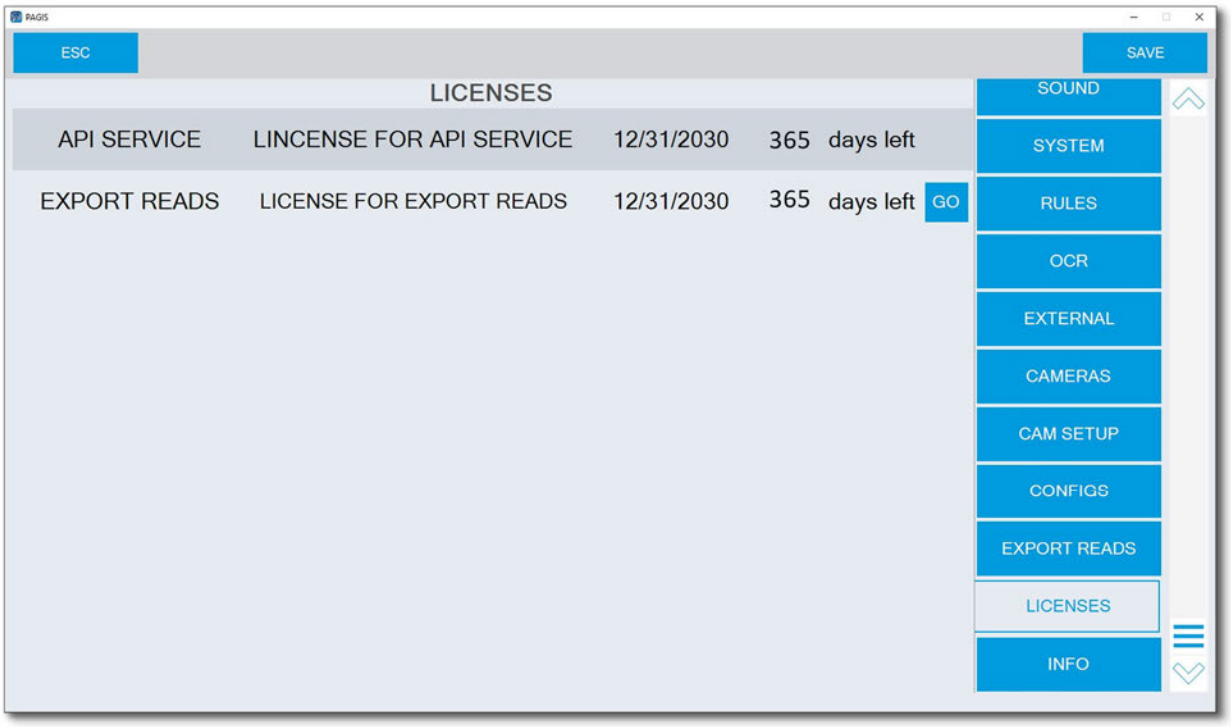
- **URL**: Specify the fully quialifed URL to the API service HTTP or HTTPS.
- **User/Password:** Set credentials for service.
- **Sync Time:** Set automatic data sync times in seconds.
- **Purge Only Synced Reads:** Prevents reads from being deleted from PAGIS regardless of back-office sync status, data will remain until synced with the RestAPI service.

2996

3.17 Licenses

PAGIS 2.15 requires Licensed activation on the following features to be activated. Once the license file is applied, PAGIS will display which feature is enabled and the time limit left on the activation. The licensing come in the form of a physical file that is coded to your DISK S/N number PAGIS is installed on. The licenses file must be place in the "C:\Program Files\PlateReader\MDC\Licenses" folder. License files are not transferable.

- **Hotlist API:** This API allows for the addition and modifications of Hotlist and Hotplates via API commands. The modifications do not apply to BOSS deployed hotlist, only for hotlist created by the API.
- **Export Reads:** Allows for the ability to export data to external RestAPI. The GO button will redirect the user to this features configuration screen.



3.18 Info

The Info screen displays additional support contact information including the PAGIS version number and OCR engine. This information is helpful when contacting Technical Support.

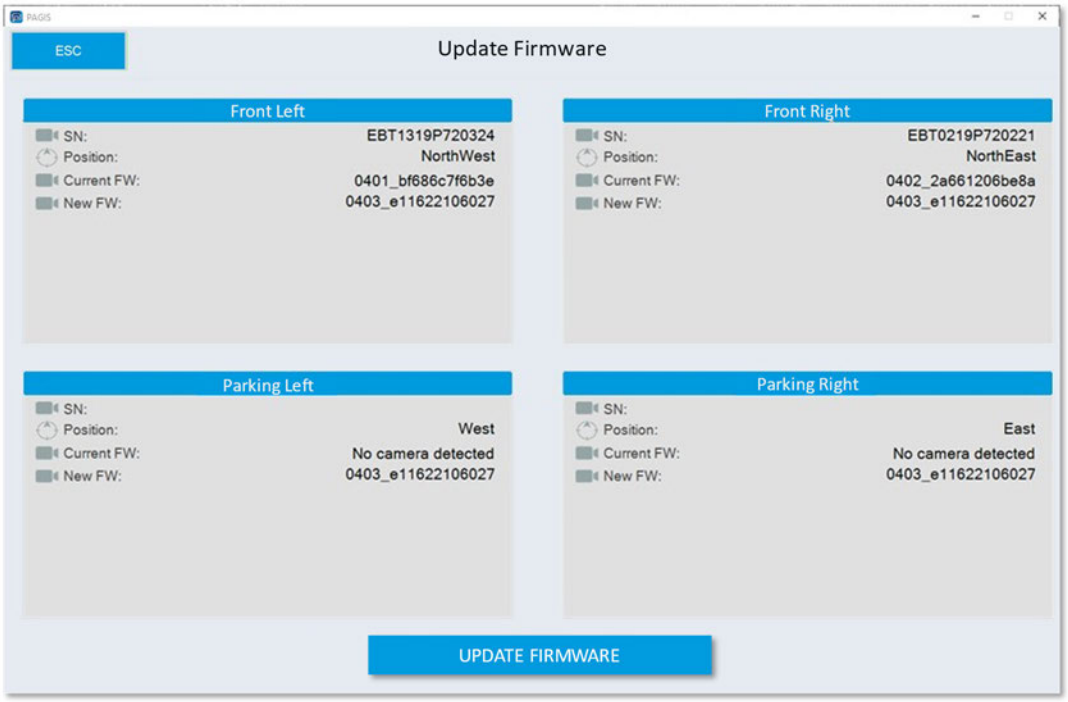


2997

3.19 Camera Firmware Update, (Admin)

Camera firmware update provides a means for Neology to update the camera software to enhance and or correct camera performance. The software nitifcation icon will only apper when a update is avialable.

- The firmware update process only updates camera that are attached and function on the mobile processor.
- Administrator must log into PAGIS and apply the FW update. *The update process takes around 4min and should not be interrupted or risk permanently damaging the cameras, PAGIS will return to normal opertaion after update.*
- Once the UPDATE FIRMWARE button is clicked PAGIS will switch to full gray screen with message indicating "**Camera Firmware is Updating**", during this process you'll will notice small command windows opening on top of PAGIS, these windows represent the firmware being applied to each active camera so you may notice one or server depending. Once completed a message will appear "**Firmware Updated Successfully**" then PAGIS will return to normal operation. *After FW completion and return to "Live View", its requiered to cycle thought the "Cam Mods" to refresh cameras.*



Firmware Updater Window List.

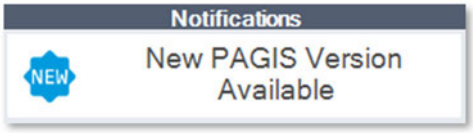
- Title "Camera Name".
- Camera serial number.
- Position.
- Current FW version.
- New FW version available.

2998

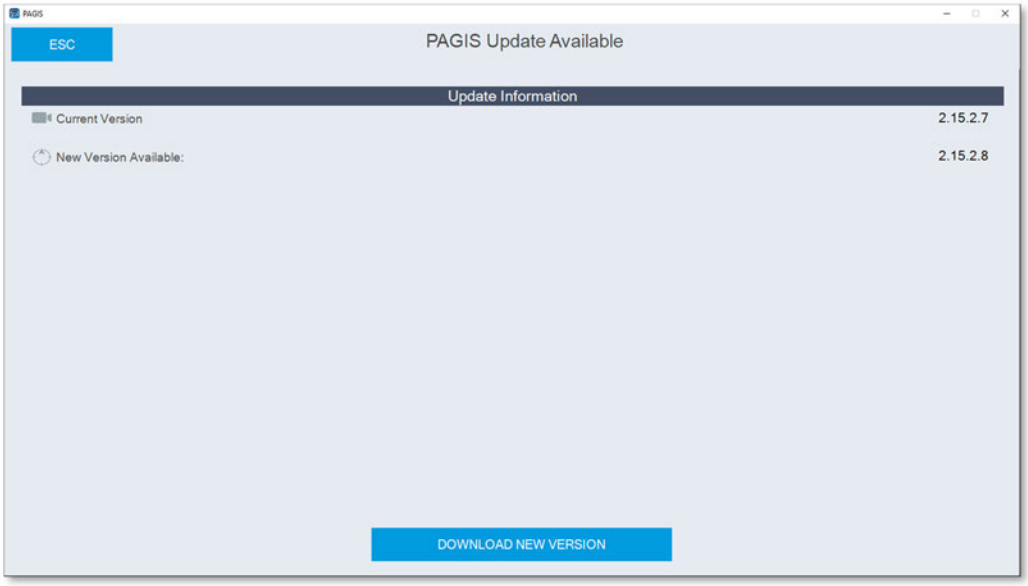
3.19.1 PAGIS Software Update, (Admin)

New in version 2.15 is the ability to remotely update the PAGIS software. Provided that the Client or Standalone PAGIS has internet access, updates are accessible.

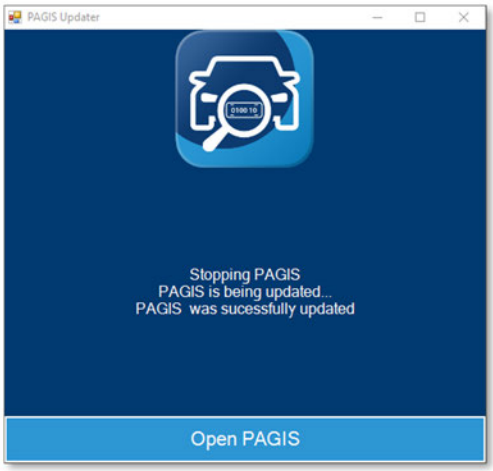
- In Client/Server confriguration the administrator must make sure that PAGIS is activly communication to the prcessor, essentaly the mobile system is in working order.
- When update avilable PAGIS will display the SW notifcation icon  in the system menu. Clicking the notifcation icon will indicate to the user weather it's a SW or FW update, for PAGIS update uniqe badge will apper indicating PAGIs has a newer version avilable.



- To continue the PAGIS update, clicking the update badge will open the update information screen indicating your current and newer version of PAGIS available.



- To start the software update, click the DOWNLOAD NEW VERSION button. PAGIS will indicate to the user that the software is updating and do not power off the system, please wait.
- Once the update is completed a new window will appear saying the update was completed successfully and give the user the option to open PAGIS.



2999

PAGIS INSTALLATION GUIDE

4.1 PAGIS System Requirements

The PAGIS Software requires the following minimum system requirements for the mobile data computer:

- Intel I3 CPU at 2.0 GHz or higher.
- Windows Operating System (Win10& 11).
- Microsoft .NET Framework 4.8.
- 8 GB of RAM.
- At least 1 GB of free disk space.
- SVGA display with a minimum resolution of 800 x 600 pixels.
- Available 10/100/1000 Ethernet port.
- Keyboard and mouse, or a touch screen monitor.
- Internet access needed for mapping and Firmware update.

4.2 PAGIS Prerequisites

Prerequisites:

1. Ability to install software.
2. Ability to configure the network adapter.
3. PAGIS 2.15 and above are only compatible with SX4 and SX4e Processors.

Network Adapter Settings:

The Neology mobile processor operates based on a static IP and is preassigned the IP address of 192.168.200.201. When connecting laptop/MDC to the mobile processor your computer must be on the same IP network as the mobile processor, in fact the connecting compute must adopt one octet lower than the assigned IP of the processor for MDC installed PAGIS to connect to the mobile processor and receive data from the ALPR cameras. Below are the steps to configure your computer.

1. Navigate to Adapter Options in Windows and right click on the adapter and select properties.
2. Click to select IPv4 and click Properties
3. Click the radio button "Use the following IP Address" to set the Static IP address.
4. Enter 192.168.200.200 in "IP address" section.
5. Enter 255.255.255.0 in "Subnet mask" section.
6. Either leave the "Default gateway" blank or enter 192.168.200.201.
7. Click OK to save changes.

NOTE: The Mobile processor is pre-configured to relay its camera data connection to the 192.168.200.200 IP address, using alternative IPs on MDC/Laptop will result in the software's failure to communicate with the cameras when using VPRelay mode.

3000

Alternative IP Network:
It is possible to configure the Neology mobile processor to utilize a different IP network in conjunction with MDC/Laptop. Typical scenario would be when mobile processor and MDC/Laptop are connected through an onboard modem that has an Ethernet switch with available ports. Below are the general steps to changing IP network.

Win10 variant of SX4e Instructions:

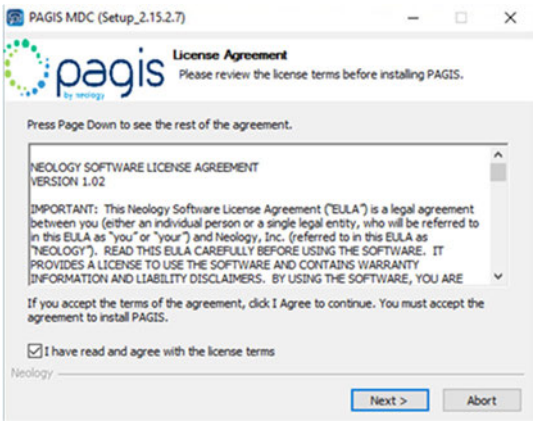
1. Follow the step above to connected to Neology mobile processor.
2. Remote desktop to Neology mobile processor and login using credentials provided in the SX4e manual.
3. In Windows "Services" find and stop the "VPRELAY" service.
4. Navigate to "D:\PlateReader\VPRelay" and located file "anpr2.ini and open in notepad.
5. Alter "Address=192.168.200.102" to the IP your MDC/Laptop will assume after change to new network, save and close. The "VPRELAY" service will use this IP address to send camera data to PAGIS running on MDC/Laptop.
6. Alter Neology mobile processors "Ethernet adapter 1" to new IP, refer to SX4e manual for instruction on disabling the "WFManager" so change made to Ethernet are permanently saved.
7. Reboot mobile processor and enable "WFManager".
8. Reassign IP on MDC/Laptop.
9. Start PAGIS on MDC/Laptop and confirm camera connectivity. Refer to FAQs in this manual for troubleshooting tips.

4.2.2 PAGIS Software Installation (MDC)

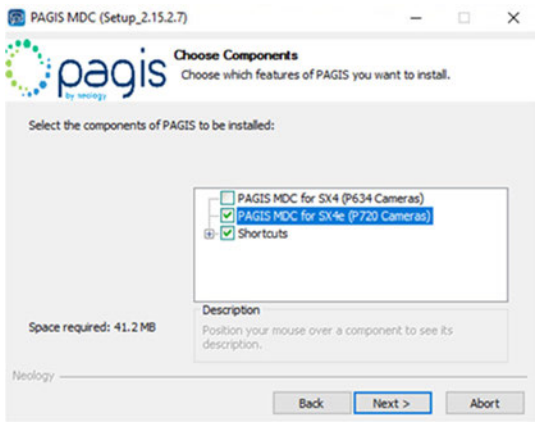
1. If PAGIS exist on your computer, it is recommended you "EndShift" any existing data, then uninstall PAGIS.
2. PAGIS 2.15 natively only supports Win10 OS versions of the SX4e mobile processor. However, it is possible to update Win7 OS version of SX4 and SX4e with PAGIS 2.15 provide some additional services are installed.
3. Upgrading to Client PAGIS 2.15 also requires that the PAGIS Service i.e. "VPRelay" on the mobile processor be updated to same version.



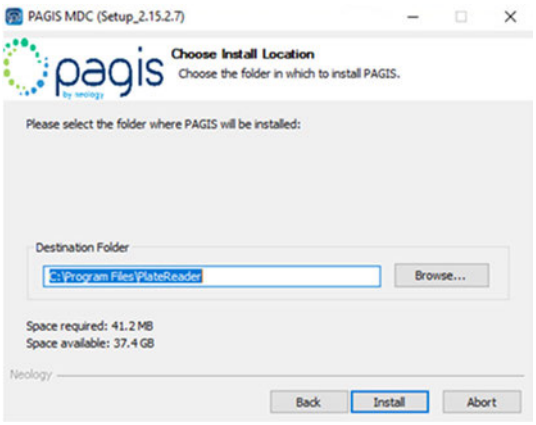
4. Place the PAGIS installer on your computer's desktop, "PAGIS_Setup_MDC_2.15.x.x.exe".
5. Right click the PAGIS installer executable and select "Run as administrator".



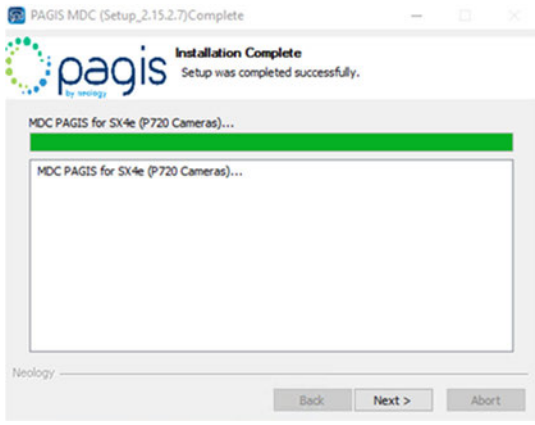
6. Check the license agreement box, then click Next.



7. Select the mobile processor type and alter "Shortcuts" if needed. Next to continue.



8. Confirm path if upgrading, click Install to proceed.



9. Installation Compete, Next to proceed.
10. Click Finish.

Note: See Appendix A for terminology definitions.

3002

4.2.3 PAGIS Software Installation (Win10 Mobile Processor)

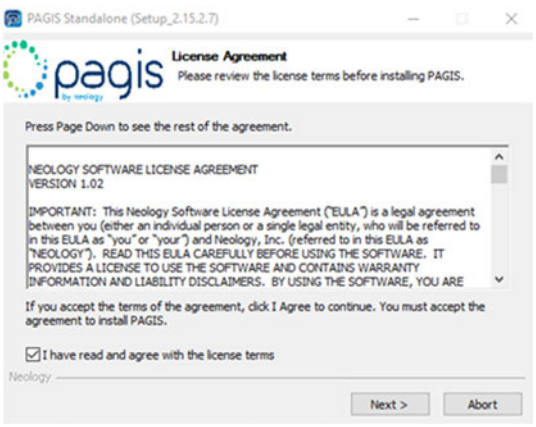
1. PAGIS 2.15 natively only supports Win10 OS versions of the SX4e mobile processor. However, it is possible to update Win7 OS version of SX4 and SX4e units with PAGIS 2.15 provide additional services are installed.
2. PAGIS can only update existing 2.15 versions of PAGIS that reside on the mobile processor. Older PAGIS versions folders should be renamed as backup.
3. The processor must be in its respective mode to update that option as the folder path is hidden when not active, see "Change Mode" in SX4e manual.

NOTE: If processor is in Service/VPRelay mode you MUST stop the "VPRELAY" service before running the updater.

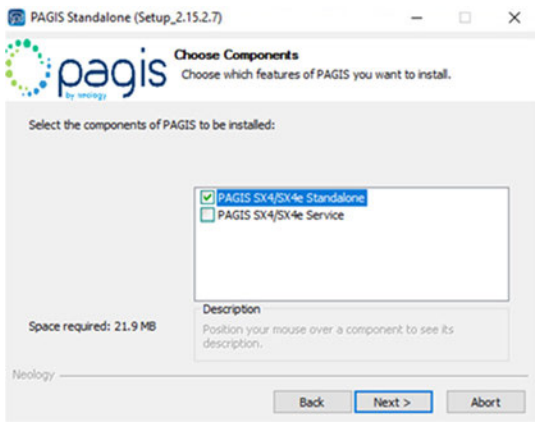
NOTE: If installing PAGIS 2.15 on any processor that was previously running PAGIS versions older than 2.15, the user MUST obtain an 64bit version of the OCR Cardet file for the cameras to operate properly. This can be accomplished by reaching out to customer support PRIOR to installation at alpr_support@neology.net.



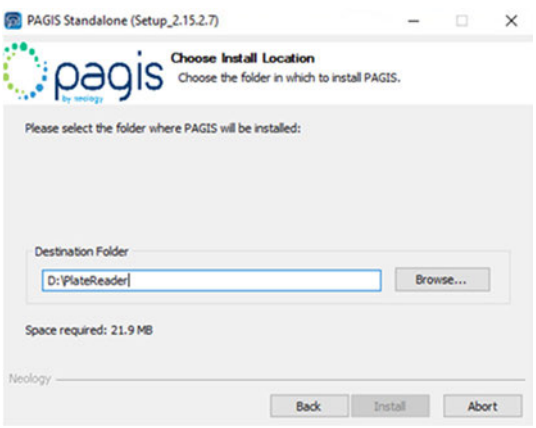
4. Remote desktop into processor or utilize attached monitor/keyboard.
5. Place the installer in D:\ drive on the mobile processor.
6. Execute PAGIS installer.



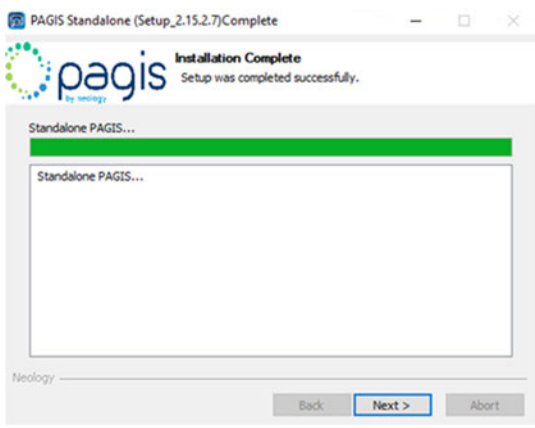
7. Check the license agreement box, then click Next.



8. Select option to update, next to continue.
   - Standalone= PAGIS login from Processor.
   - Service= PAGIS login from connected Laptop.



- Accept the default path for Win10 OS version of SX4e.
- Win7 path is "C:\PIPSTechnology"



9. Installation Compete, Next to proceed.
10. Click Finish.

Note: See Appendix A for terminology definitions.

3003

4.2.4 PAGIS Software Installation (Win7 Mobile Processor)

PAGIS 2.15 requires .NET 4.8, C++ & updated drives that are not natively present in Windows 7 processors, the following components need to be added before PAGIS 2.15 will work correctly.

1. The WFManger write protection on the processor must be "DISABLED" prior to installing the below items, see the appropriate processor SX4 or SX4e for instructions.
2. Install .NET 4.8 "**ndp48-x86-x64-allos-enu.exe**". https://go.microsoft.com/fwlink/?linkid=2088631
3. Install C++ Ver 14.28 or newer "**VC_redist.x64.exe**". https://aka.ms/vs/17/release/vc_redist.x64.exe
4. Install Drivers "**WDT_DIO_Setup_v2.2.9.1(x64).**exe" or newer. https://www.neousys-tech.com/en/support-service/resources/category/57-nuvo-2000-driver?download=319:wdt-dio&start=10
5. The user MUST obtain an 64bit version of the OCR Cardet file for the cameras to operate properly. This can be accomplished by reaching out to customer support PRIOR to installation at alpr_support@neology.net.
6. In all component installations, follow the default prompts they provide to install the programs.
7. Once all the addtinal components are installed, restart the processor.
8. Install PAGIS 2.15 as described in section 4.2.3.
9. MAKE SURE you have added the 64bit version of the Cardet file to either the VPRelay or Standalone folder on the mobile processor, depending on which operational mode you're using.
10. Once PAGIS operation is confirmed, re-enable the WFManger write protection.

3004

TROUBLESHOOTING TIPS

This section provides some basic troubleshooting tips and information

5.1 Troubleshooting & Tips

- The first login to PAGIS after the new install of an unconfigured version does not require a username or password. Simply click Login to be granted Admin access to the software.
- A good means to testing the communication from the MDC to BOSS is to telnet (over TCP 8092) via command prompt.
- A good means to testing the communication from the MDC to the SX Processor is to telnet (over TCP 9000) via command prompt.
- For many other troubleshooting tips, see Appendix C – Frequently Asked Questions

5.1.1 PAGIS with NetMotion VPN

Agencies utilizing NetMotion VPN software on the MDC will need to apply the following passthrough steps:

1. Login to the NetMotion server as administrator
2. Click Settings > Then select Client > Select Global Client Settings > Then select Passthrough List
3. Click the "Add..." button on the right > Select "Network Address"
4. Enter the following settings (as shown):
    A. IP address:192.168.200.0 (the zero is correct, it's an IP address "range") Subnet Mask: 255.255.255.0.
    B. Keep all other settings default (as shown) and click OK.
5. The MDC must then disconnect from NetMotion and reconnect again for the settings to be applied locally.

5.1.2 Cisco VPN Client:

Make sure Stateful Firewall is unchecked and "Allow Local LAN". If utilizing

5.1.3 Microsoft .NET 4.8 or newer Installation

The PAGIS 2.15 Software requires *Microsoft .NET Framework 4.8* or newer. If the MDC doesn't have .NET, it can be downloaded from the Microsoft website.

5.1.4 Firewall Settings for Client-Server Installations

For client-server installations, the Windows Firewall needs to allow the SX Processor and the MDC to communicate. If the MDC is maintained by a Network Administrator, he or she should be contacted before making changes to the firewall. The command prompt commands for the exceptions are below

Option 1: Allow Microsoft Windows Version 8 or newer to auto-detect the launch of the PAGIS.exe application and use the wizard to add the PAGIS.EXE to the exception list (making note of Public or Private Network settings as necessary).

Option 2: Add PAGIS to the exception list manually by browsing to the install path of PAGIS. The default is below for reference: "C:\Program Files\MDC\PAGIS.exe".

Option 3: Add the communication ports manually:
TCP in/out 8092 = Pagis sync port to BOSS back-office software.
TCP in/out 9000 = Mobile processor camera feed port.
TCP in/out 9001 = Mobile processor camera snapshot port.
TCP in/out 32023 = Mobile processor camera setup port.
TCP in/out 10000 = Mobile processor data capture port.
NOTE: XML Datastream uses TCP 10100 and TCP 7000

3005 PAGIS/BOSS4 CONFIGURATION

For PAGIS to function properly, it must have an open network connection to the host back office.

6.1 Creating a New Device in BOSS4

Once network communication to BOSS4 has been established from the vehicle, a new device must be "built" or added to the Device List in BOSS4 before it can be used. The approved way to do this, is to simply perform a Begin Shift from the PAGIS software. NOTE: The computer name is what will be displayed in BOSS as device name.

1. At the PAGIS Live View Screen, click the Begin Shift button to launch a manual the sync.
2. If the computer has previously been setup to communicate with BOSS and is already enabled, the sync transfer window should appear in the middle of the Live View Screen.
3. If this is a new/disabled device, a message indicating "HttpStatusCode Unauthorized" will be displayed. This indicates the BOSS4 server has received the sync request but has rejected it due to device status.
4. Once the BOSS Admin has enabled the device, the Status Code error will not appear again, and syncs should complete as configured in BOSS4.

6.2 Enabling a New Mobile System in BOSS4

Installing PAGIS and configuring the network settings is only the first step in making the ALPR unit operational. Once PAGIS is configured to work with or on the SX Processor and the mobile cameras, it must then be enabled in BOSS4 before synchronizations can take place. NOTE: By default, every new device recognized by the BOSS4 server is disabled until the admin enables it. This is done for security reasons to prevent unauthorized communications.

1. Log into the BOSS4 URL with Admin privileges and navigate to the Resources pulldown menu.
2. Find the Devices from the menu options. The new device should now be listed.
3. Click the Enable slide toggle to enable device, located in the same row in column title "Enabled".
4. This will enable the device, synchronization between BOSS4 and PAGIS is allowed.

NOTE: Once the Device is enabled the admin needs to assign Users and Hotlist distribution.

6.3 Assigning Ownership to a Device in BOSS4

Every new device added to BOSS4 allows for Admin level access into PAGIS without the use of a username or password. To password protect the PAGIS software, the BOSS Administrator must deploy Users and or Groups of Users to the new device in BOSS4.

NOTE: For more detail on Users, User Groups, Sites, and Roles, refer to the BOSS4 manual.

1. Login to the BOSS4 URL with Admin credentials and navigate to the Resources pulldown menu.
2. Select Devices from the menu options. The new device should now be listed.
3. Click the name of the Device to select it. (This will open the device details windows on the left)
4. Locate the "Groups and Users" button and a list of all available Groups of Users will appear.
5. Select the users to be assigned to the device.
6. Click the Save button at the bottom right of the Edit window.

6.4 Assigning Hotlists to a Device in BOSS4

For the PAGIS users to receive alerts, one or more of the stored hotlists in BOSS4 must be distributed to the new device. NOTE: For more information on building and configuring Hotlists, refer to the BOSS4 manual.

1. Login to the BOSS4 URL with Admin credentials and navigate to the Resources pulldown menu.
2. Select Devices from the menu options.
3. Click the Deployment hotlist button and select the desired hotlist to be deployed.
4. Click the Save button at the bottom right of the Edit window.

3006

APPENDIX A: THE GLOSSARY

ALPR/ANPR	"Automatic License Plate Recognition/Automatic Number Plate Recognition".
BOSS	"Back Office System Software". This is the ALPR server.
GPS	"Global Positioning System".
GUI	"Graphical User Interface".
Hotlist	A database or list that contains vehicle license plates of interest ("alert list").
IR	Infrared light.
License Plate	Also called a tag or number plate.
MDC	"Mobile Data Computer". This is the tablet or laptop in the vehicle.
OCR	"Optical Character Recognition" (also referred to as a "cardet").
OS	"Operating System".
PAGIS	This is the License Plate Capture Software most commonly used in an ALPR vehicle.
Service	Operation mode of the PAGIS software. Service or "VPRelay" is used to refer to PAGIS instance that is running directly on the Neology mobile processor without a GUI interface, this mode is intended to run in conjunction with MDC version of PAGIS installed on laptop connected via Ethernet.
Standalone	Operation mode of the PAGIS software. Standalone is used to refer to PAGIS instance that is running directly on the Neology mobile processor with a GUI interface. Same a "Service"
SX	SX is a short notation referencing Neology mobile processor, commonly the SX is followed by the generation number of the processor, i.e. SX3, SX4 & SX4e.
UI	A "User Interface" is the means in which the user can access and navigate the software.
USB Flash Drive	Also called a thumb drive or memory stick.
VLP	"Vehicle License Plate".
VPN	"Virtually Protected Network".
VPRelay	Operation mode of the PAGIS software. VPRelay or "Service" is used to refer to PAGIS instance that is running directly on the Neology mobile processor without a GUI interface, this mode is intended to run in conjunction with MDC versions of PAGIS installed on laptop connected via Ethernet.
Whitelist	Opposite of a standard BOSS Hotlist. This is a list of license plates that should not trigger an alert.

APPENDIX B: PAGIS SOFTWARE DATABASE FILE

This section is used to configure the PAGIS Software when it's not being used with the Back Office System Software (BOSS). Comma-separated value (CSV) format is the only format the PAGIS Software supports for importing data into the vehicles for the purpose of matching against the captured license plate data. PAGIS will support CSV files with any number of columns, called "fields", as long as the first field is the VLP (Vehicle License Plate). NOTE: The CSV format is standard ASCII.

Example CSV Files:

1. *ABC123, Red, Ford, Explorer, 1996, WANTED XYZ456, Blue, Audi, A4, 2001, MURDER*
2. *45ABC234, Vehicle wanted in associated with a kidnapping on 12/5/2005 995BD233, Vehicle reported stolen from Liz's Lounge at 6am on 12/1/2005*
3. *UIO223 ABC123*

General Function:

PAGIS calls/utilizes files in pairs. Each database in PAGIS is created using two files: a CSV file, and an INI configuration file. Without both files, the database will not load and PAGIS will not "see" it. Each CSV file/hotlist must have the exact same name as the INI configuration file. Example: Stolen.ini and Stolen.csv will work. Stolen.ini and Plates.csv will not.

Reading an INI Configuration File

Lines that appear in brackets [] are called "Headings". The labels that appear inside the headings, are called "values". Values will always contain an equal sign (=). If a line starts with a semicolon, it is a comment and is not read by the software. There is no limit to the number of comments in the INI file.

The [SETTINGS] Heading

The values in the Settings heading are: NumFiles, DbName, DbColor, Priority, Covert, Alarm, and NumFields.

- NumFiles: Determines how many database files the system should split the specified hotlist into. Generally, this value is set to 1. But for larger hotlists (200,000+ lines), a number of 2-5 may be more desirable.
- DbName: Tells the PAGIS Software what the displayed name of the hotlist should be.
- DbColor: Sets the display color of the hotlist. This is merely an esthetic setting and not a functional setting. The right-hand side of the equal sign is the HEX value representing the ARGB values for the color. If this value is unknown, the admin should simply leave this line out of the file.
- Priority: Designates the priority of this hotlist in relation to other hotlists in the system. The highest priority database is 1 and the lowest is 999. NOTE: if a plate resides on multiple lists the higher priority will be alerted first.
- Covert: Determines whether standard PAGIS Software users are alerted when a hit is made from the database. Covert database can be used for hotlists that are included for information-gathering purposes rather than eliciting user intervention. The system can also be configured to notify via email or SMS message when a hit is made from a covert hotlist.
- Alarm: Sets the audible alert to be played in PAGIS when a hit is made from the hotlist. Values for Alarm are LOW, MED, HIGH
- NumFields: Indicates how many fields (columns) are in the CSV file. If this value is less than the actual number of fields in a file, then the additional fields are placed in the general information area. This value also determines the number of headings of the [Field x] present in the file. For example, if NumFields=2 then there will be two additional headings, [Field 0] and [Field 1]. NOTE: Adding "Creation =" will place the timestamp the hotlist was added to the Begin Shift file.

3008

The [FIELD X] Heading

Under the Field heading, there are two configurable values, "Name" and "PAGIS".

- Name: Tells the system what the name of this field is. If no name is specified, then no name given to the field. The format is Name = <field>
- PAGIS: Specifies how to display the field in the GUI/PAGIS Software.
    - If no value is defined, the field is placed as general information.
    - Values 1-5 represent special fields for the PAGIS Software that translate to the information being displayed in a box of its own when a hit is processed.
    - A value of 6 represents an ID number to cross reference the vehicle from the hotlist with a person from the wanted list.
    - A value of 7 is identical to leaving the value undefined.

Sample INI Configuration File

[Settings] NumFiles=1
DbName=Stolen Vehicles DbColor=ffffff00 Priority=5 Covert=False Alarm=MED NumFields=8
;PAGIS Values
;0 is VRM / VLP (Not User Definable, always Field 0)
;1 is Special Field 1
;2 is Special Field 2
;3 is Special Field 3
;4 is Special Field 4
;5 is Special Field 5
;6 is ID Number (PNC ID, Driver's License, Social Security Number, etc.)
;7 is General Info (Default for all undefined fields) [Field 0]
PAGIS=VRM

Sample INI Configuration File

[Field 0] Name=VRM
[Field 1] Name=Color
PAGIS=3 [Field 2]
Name=Make PAGIS=1
[Field 3] Name=Model
PAGIS=2 [Field 4]
Name=Action PAGIS=4
[Field 5] Name=Warning
PAGIS=5 [Field 6]
Name=PNCID PAGIS=6
[Field 7] Name=Intelligence PAGIS=7

To deploy a locally created hotlist to PAGIS without BOSS.

1. Create a folder called "beginshift" (Without Quotes) on the root drive of whatever drive media you're using that PAGIS has access to, remember only on root drive, no subdirectories. Example C:\beginshift.
2. Place the .CSV & .INI in the newly created beginshift folder.
3. Log into PAGIS and configure Sync to access the drive where your file/files are located. When setting disk drive letter in PAGIS no need to indicate folder path as PAGIS assumes by default that "beginshift" exist on the root drive your selecting, refer to section 3.1 in this manual.
4. Go back to main screen and do beginshift.

3009

APPENDIX C: XML DATASTREAM

Overview

The XML Datastream can be used to push the current data from a running PAGIS system to another application. The data available via the Datastream includes reads, hits, and current images. The connection to the Datastream is a TCP/IP socket (default ports: 10100 & 7000). When initially connecting, an XML packet is passed to the PAGIS Software to subscribe to the Datastream. The data connection is configured as "push only" and doesn't allow receipt of additional external data. The current image stream is pushed periodically whereas reads and hits are passed as close to real-time as possible.

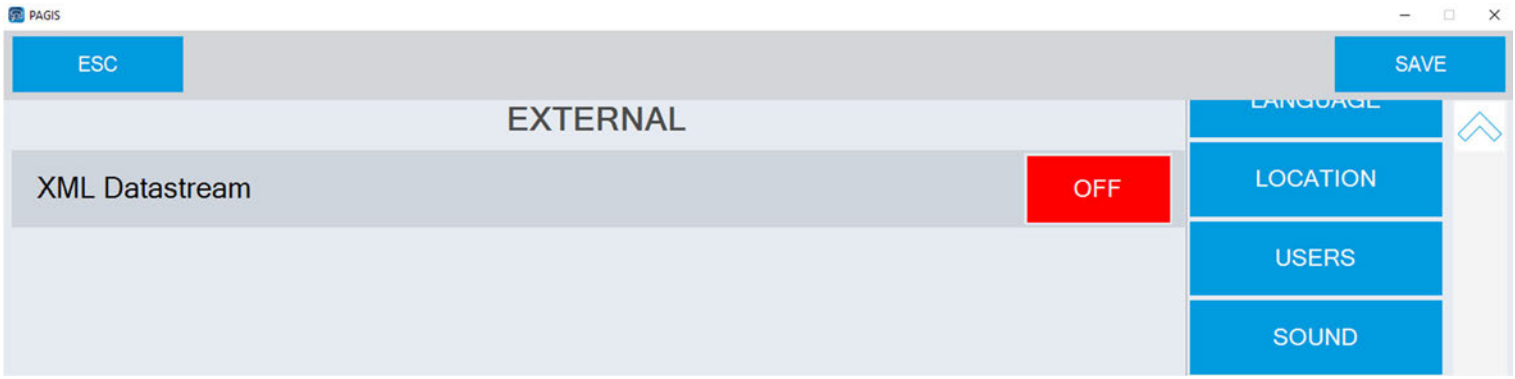
PAGIS Port

By default, the PAGIS.exe.config file has a key for defining the port number for the XML Datastream. The default value is 10100 & 7000. This setting does not need to be changed unless the default ports are unavailable.
The key has the following format:

```
<!--XML Datastream Settings/-->
        <add key="External.TCP.Querier.Port" value="7000" />
        <add key="XML.Datastream.Port" value="10100" />
```

PAGIS Admin Setting

To utilize this feature, the XML Datastream needs to be enabled in PAGIS. To do this, navigate to Settings > Admin > External. The "XML Datastream" option should be turned on as shown in the image below and then saved.



XML Subscription

When initially connecting to PAGIS, the Datastream subscriber will receive only a Heartbeat XML packet (see example below) until PAGIS receives a subscription packet from the subscriber. The properly formed subscription packet defines the specific data that the subscriber wishes to receive.

Heartbeat XML Packet

The Heartbeat Packet is sent once every 10 seconds. The purpose of the heartbeat packet is to let the subscriber know that the communications channel is working between PAGIS and the subscriber. The timestamp is sent in the format of "`YYYY-MM-DDThh:mm:ss`".

Sample of the Subscription XML Packet

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-heartbeat>
  <timestamp>2011-10-13T09:41:56Z</timestamp>
</pips-datastream-heartbeat>
```

3010

Subscription XML Packet

A properly formed subscription packet will have all the data being requested from PAGIS. To receive a specific datatype, a tag must be added to the subscription to define the desired datatype. The valid entries for datatype are: Reads, Hits, and Current Image.

- Subscribing to Reads will send all plates that are detected by PAGIS regardless of whether it has an associated hit.
- Subscribing to Hits will send all plates detected by PAGIS that are on a hotlist and the associated Read data for that Hit.
- Subscribing to the Current Image Datastream offers two additional attributes that may be passed as well. The "camera" attribute can be set to determine which camera the image is coming from. If no value is passed for "camera" the value defaults to zero. The "milliseconds" attribute determines how long the system waits between sending the current image. The default value for milliseconds is 1000. If a value of zero is sent, the system will send a single snapshot.

Sample of the Subscription XML Packet

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-subscription>
  <datatype>Reads</datatype>
  <datatype>Hits</datatype>
  <datatype>HitTrigger</datatype>
  <datatype camera="0" milliseconds="1000">CurrentImage</datatype>
</pips-datastream-subscription>
```

Hit Trigger

The HitTrigger packet is used to alert other systems that a hit has occurred on the PAGIS system. The packet is greatly simplified from the Reads/Hits XML packet and only contains the license plate text, timestamp, and a description of the hit. The description will contain the name of the hotlist that originated the hit and may be used to send additional information.

Sample of the HitTrigger XML Packet

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-hittrigger>
  <timestamp>2011-10-13T09:41:56Z</timestamp>
  <vrm>SBX989</vrm>
  <hotList name='Alpha'>
    <field1><![CDATA[This is Alpha Field 1]]></field1>
    <field2><![CDATA[This is Alpha Field 2]]></field2>
    <field3><![CDATA[This is Alpha Field 3]]></field3>
    <field4><![CDATA[This is Alpha Field 4]]></field4>
    <field5><![CDATA[This is Alpha Field 5]]></field5>
  </hotList>
</pips-datastream-hittrigger>
```

Reads/Hits XML Packet

The Reads/Hits packet contains information about the plate that was detected. This information includes:

- Source – The device that detected the plate
- Camera – The camera on the device that detected the plate
- Read – The Information about the plate that was captured
- VRM – The plate translated to text
- Timestamp – When the read occurred
- GPS – The location coordinates where the read took place
- ImagesPatch – The image of plate in infrared (IR)
- Overview – The image of scene/car in Color
- Hits – The associated hotlist(s) data

3011

Sample of the Current Image XML Packet

NOTE: The Current/Live Image XML Packet contains the current image from the camera. It is sent every 5 seconds.

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-currentimage>
  <timestamp>2011-10-13T09:41:56</timestamp>
  <data>(Image data here)</data>
</pips-datastream-currentimage>
```

Sample Read with Hits XML

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-reads>
  <reads>
    <source>
      <name>PAGIS_90210</name>
      <software name="PAGIS" version="2.6.8" />
      <camera name="Front Left">
        <read>
          <state>TN</state>
          <vrm>SBX989</vrm>
          <confidence>97.5</confidence>
          <timestamp>2011-09-30T09:30:10Z</timestamp>
          <username><![CDATA[shronski]]></username>
          <gps>
            <latitude>-87.4567</latitude>
            <longitude>98.7654</longitude>
          </gps>
          <images>
            <image name='Patch'>
              <type>IR</type>
              <data>

<![CDATA[/9j/4AAQSkZJRgABAQAAAQABA.....................................................................................
..................................................................................... /9k=]]>
              </data>
            </image>
            <image name='Overview'>
              <type>Color</type>
              <data>

<![CDATA[/9j/4AAQSkZJRgABAQAAAQABAAD.................................................................................
..................................................................................... //2Q==]]>
              </data>
            </image>
          </images>
          <misread>0</misread>
          <manual>0</manual>
          <hits>
            <hotList name='Alpha'>
              <field1><![CDATA[This is Alpha Field 1]]></field1>
              <field2><![CDATA[This is Alpha Field 2]]></field2>
              <field3><![CDATA[This is Alpha Field 3]]></field3>
              <field4><![CDATA[This is Alpha Field 4]]></field4>
              <field5><![CDATA[This is Alpha Field 5]]></field5>
            </hotList>
            <hotList name='Beta'>
              <field1><![CDATA[This is Beta Field 1]]></field1>
              <field2><![CDATA[This is Beta Field 2]]></field2>
              <field3><![CDATA[This is Beta Field 3]]></field3>
              <field4><![CDATA[This is Beta Field 4]]></field4>
              <field5><![CDATA[This is Beta Field 5]]></field5>
            </hotList>
          </hits>
        </read>
      </camera>
    </source>
  </reads>
</pips-datastream-reads>
```

3012

APPENDIX D: Hotlist API

Overview

Hotlist API allows for the addition and modifications of Hotlist and Hotplates via API commands. The modifications do not apply to BOSS deployed hotlist, only for hotlist created by the API.

1. API features only applies to PAGIS version 2.15.2.5 and newer. This newer version of PAGIS includes the first version of the licensing which we can enable or disable the Hotlist API feature.
2. We generate the license using the serial number of the disk PAGIS is running from. That value can be obtained from the PAGIS interface by clicking twice on the version number at the login screen or in the system status view in the software, CTRL-C to copy the S/N into clipboard.
3. Send the captured disk S/N into Neology support at alpr_support@neology.net, titling your request as "PAGIS API License Request" and you must reference a case# or customer the request is linked to.
4. The license should be placed in the Licenses Folder in the PAGIS Directory, PAGIS will read that file and enable the API service.
5. Future licensing features will have the option to enable specific features in the API.

This API includes the following methods to add, remove or modify PAGIS Hotlist and Hotplates databases.

- The API is run locally in PAGIS, once it's started.
- API exposed port is TCP/IP 8080.
- Port number used can be changed by editing the PAGIS file "PAGIS.exe.config" file in section <configurations> under <appsettings>, value is <add key="APIPort" value="8080" />.
- HTTP request URL syntax is http://127.0.0.1:8080/api/v1/hotlist, this URL can also be used in a browser to initially test if API is operational.

  Hotlist:
  - GET (return all hotlists or one)
  - POST (Insert Hotlist)
  - PATCH (Update hotlists content partially)
  - PUT (Update entire content of hotlists)
  - DELETE (Remove Hotlists from database)

  Hotplates:
  - GET (return all hotplates or one from a specific hotlist)
  - POST (Insert Hotplates in a hotlist)
  - PATCH (Update hotplate content partially from a specific hotlist)
  - PUT (Update entire hotplate content from a specific hotlist)
  - DELETE (Remove Hotplate from a specific hotlist)

3013

API Hotlists Commands

Process hotlists information stored in PAGIS

1.1 GET Hotlists

Summary GET Hotlists:	
Service Name	**getHotlists**
URL	**/api/v1/hotlists**
Description	**This method returns all hotlists stored in PAGIS database.**

Parameters: = No parameters

Responses:

Code	Description

201	{
	"Data": [
	{
	"Id": 3,
	"Name": "Stolen Vehicles",
	"Color": "#2A4454FF",
	"Alarm": "MED",
	"Priority": 100,
	"Timestamp": "637822639495249351",
	"isCovert": false,
	"isExternal": false,
	"isWhitelist": false,
	"type": 0
	}
	]
	}

500	**Internal Server Error**

3014

1.2 POST Hotlists:

Summary POST Hotlists:	
Service Name	**addHotlist**
URL	**/api/v1/hotlists**
Description	**Insert a new hotlist to PAGIS database**

Parameters:	
Name	**Description**

HotlistsItem (body)	<pre>{
	  "Name": "Stolen Vehicles",
	  "Color": "#2A4454FF",
	  "Alarm": "MED",
	  "Priority": 100,
	  "Timestamp": "637822639495249351",
	  "isCovert": false,
	  "isExternal": false,
	  "isWhitelist": false,
	  "type": 0,
	  "Id": 54
	}</pre> **Parameter content type: application/json**

Note: the "Timestamp" variable, regardless of value set, the timestamp in PAGIS will read 1/1/1753. You must use the PATCH hotlist command to update timestamp, typically after adding hotplate.

Responses:	
Code	**Description**
201	**Hotlist created**
500	**Internal Server Error**

1.3 PUT Hotlists

Summary PUT Hotlist	
Service Name	PUTHotlist
URL	/api/v1/hotlists
Description	Update entire hotlist content

Parameters:

Name	Description

HotlistsItem (body)	{
	"Id": 3,
	"Name": "Stolen Vehicles",
	"Color": "#2A4454FF",
	"Alarm": "MED",
	"Priority": 100,
	"Timestamp": "637822639495249351",
	"isCovert": false,
	"isExternal": false,
	"isWhitelist": false,
	"type": 0
	}
	Parameter content type: application/json

Responses:

Code	Description
200	Hotlist Updated
404	Hotlist does not exist in PAGIS database
500	Internal Server Error

1.4 GET Hotlist

Summary GET Hotlists:	
Service Name	GetHotlist
URL	/api/v1/hotlists/{id}
Description	Get hotlist content from ID

Parameters:	
Name	Description
Id *required *Integer* (Path)	Identifier of the hotlist

Responses:	
Code	Description

200	• {
	"Data": {
	"Name": "Stolen Vehicles",
	"Color": "#2A4454FF",
	"Alarm": "MED",
	"Priority": 100,
	"Timestamp": "637822639495249351",
	"isCovert": false,
	"isExternal": false,
	"isWhitelist": false,
	"type": 0
	}
	}

404	Hotlist does not exist in PAGIS database
500	Internal Server Error

3017

1.5 PATCH Hotlist

Summary PATCH Hotlists:	
Service Name	**PatchHotlist**
URL	**/api/v1/hotlists/{id}**
Description	**Modifies partial content of hotlist stored in PAGIS database**

Parameters:	
Name	**Description**
Id *required ***Integer** **(Path)**	**Identifier of the hotlist**

HotlistsItem
(body)
	Hotlist item parameters to update
	• {
	"Color": "#2A4454FF",
	"Alarm": "MED",
	"Priority": 100
	"Timestamp": "5/26/2022 4:11:11 PM"
	}
	Parameter content type: text/plain

Note: Please note the time/date format to use when updating the "Timestamp"

Responses:	
Code	**Description**
200	**Hotlist was modified**
404	**Hotlist does not exist in PAGIS database**
500	**Internal Server Error**

3018

1.6 Delete Hotlist

Summary DELETE Hotlists	
Service Name	DeleteHotlist
URL	/api/v1/hotlists/{id}
Description	Deletes hotlist stored in PAGIS database from id

Parameters:	
Name	Description
Id *required *Integer* (Path)	Identifier of the hotlist

Responses:	
Code	Description
200	Hotlist was deleted
404	Hotlist does not exist in PAGIS database
500	Internal Server Error

API Hotplate Commands

Process hotplate information stored in PAGIS

2.1 GET Hotplates

Summary GET Hotplates	
Service Name	**getHotplates**
URL	**/api/v1/hotlists/{hotlistId}/hotplates**
Description	**The user can get all hotplates stored in a specific hotlist.**

Parameters:	
Name	**Description**
HotlistId *required ***Integer*** **(Path)**	**Identifier of the hotlist**

Responses:	
Code	**Description**

200	{
	"Data": [
	{
	"Id": 32,
	"VRM": "ABC123",
	"Field1": "Toyota",
	"Field2": "Corolla",
	"Field3": "2016",
	"Field4": "Red",
	"Field5": "CA",
	"PNCID": "13123",
	"Information": "Stolen vehicle",
	"BOSSID": " "
	}
	]
	}

404	**Hotlist does not exist**
500	**Internal Server Error**

3020

2.2 POST Hotplate

Summary POST Hotplates	
Service Name	**AddHotplates**
URL	**/api/v1/hotlists/{hotlistId}/hotplates**
Description	**The user can insert a hotplate into a hotlist**

Parameters:	
Name	**Description**
HotlistId *required ***Integer** **(Path)**	**Identifier of the hotlist**

hotplates
(body)
	{
	"hotplates":[
	{
	"VRM": "ABC123",
	"Field1": "Toyota",
	"Field2": "Corolla",
	"Field3": "2016",
	"Field4": "Red",
	"Field5": "CA",
	"PNCID": "13123",
	"Information": "Stolen vehicle",
	"BOSSID": 114
	}
	]
	}
	Parameter content type: application/json

Responses:	
Code	**Description**
200	**Hotplate Inserted**
404	**Hotlist does not exist**
500	**Internal Server Error**

3021

2.3 GET Hotplate

Summary GET Hotplates	
Service Name	**GetHotplate**
URL	**/hotlists/{hotlistId}/hotplate/{hotplateId}**
Description	**The user can get the hotplate stored in a specific hotlist**

Parameters:	
Name	**Description**
HotlistId *required ***Integer*** **(Path)**	**Identifier of the hotlist**
HotplateId *required ***Integer*** **(Path)**	**Identifier of the Hotplate**

Responses:	
Code	**Description**

200	{
	"Data": {
	"Id": 32,
	"VRM": "ABC123",
	"Field1": "Toyota",
	"Field2": "Corolla",
	"Field3": "2016",
	"Field4": "Red",
	"Field5": "CA",
	"PNCID": "13123",
	"Information": "Stolen vehicle",
	"BOSSID": " "
	}
	}

404	**Hotlist does not exist**
500	**Internal Server Error**

3022

2.4 PATCH Hotplate

Summary PATCH Hotplates	
Service Name	**PatchHotplate**
URL	**/hotlists/{hotlistId}/hotplate/{hotplateId}**
Description	**Modifies partial content of hotlplate stored in PAGIS database**

Parameters:	
Name	**Description**
HotlistId *required ***Integer*** **(Path)**	**Identifier of the hotlist**
HotplateId *required ***Integer*** **(Path)**	**Identifier of the Hotplate**

**HotlistsItem
(body)**
	Hotplate parameters to update
	{
	"Field1": "Toyota",
	"Field2": "Corolla",
	"Field3": "2016"
	}
	Parameter content type: text/plain

Responses:	
Code	**Description**
200	**Hotplate was modified**
404	**Hotlist or hotplate does not exist in PAGIS database**
500	**Internal Server Error**

3023

2.5 Delete Hotplate

Summary DELETE Hotplates	
Service Name	DeleteHotplate
URL	/api/v1/hotlists/{hotlistId}/hotplate/{hotplateId}
Description	Deletes hotlplate from a specific hotlist stored in PAGIS database.

Parameters:	
Name	Description
HotlistId *required *Integer* (Path)	Identifier of the hotlist
HotplateId *required *Integer* (Path)	Identifier of the Hotplate

Responses:	
Code	Description
200	Hotplate was Deleted
404	Hotlist or hotplate does not exist in PAGIS database
500	Internal Server Error

3024

2023 AXON ROADSHOW

The Axon Roadshow is coming! Axon is excited to visit your area as part of our 2023 Axon Roadshow. Join us for a day of low-stress demos and of course some free lunch and swag–see you on the road!

TUESDAY – OCTOBER 31ST 10:00 AM – 2:00 PM

HOST:
Plymouth Police Department

LOCATION:
20 Long Pond Rd, Plymouth, MA 02360

- **VIRTUAL REALITY**
- **TASER 7**
- **AXON BODY 3**
- **EVIDENCE.COM**
- ***TASER 10**

- **AXON AID**
- **CAMERA MOUNT SWAP**
- **FLEET 3 + ALPR**
- **AXON AIR/DRONES**
- **AXON BODY 4**

** COME EXPERIENCE THE START OF A NEW ERA IN LESS-LETHAL TECHNOLOGY. DEPLOY A TASER ENERGY WEAPON AT NEARLY DOUBLE THE DISTANCE OF OUR PREVIOUS WEAPONS.*

WHO SHOULD ATTEND:

If you work in Law Enforcement, Fire, EMS, Corrections, Public Safety, and local government, we encourage you to attend. Roadshow events give you hands-on time with technology built to make you and your community safer.

For more information contact: roadshow@axon.com







PRE-REGISTER TODAY

PRE-REGISTER TODAY TO RECEIVE A SPECIAL ITEM AT CHECK-IN!

VerizonFrontline

AXON

FY23 April Invoice for Department of Police

Charge Summary

MMARS Code	Description		Amount
BCS	Computer Resources (ChargeBack)	$	186,229.15
PAD	FOR THE PURCHASE & HANDLING OF SUPPLIES	$	199.06
PAS	Tech Services Pass Through	$	3,117.82
Total:		$	189,546.03

Document ID Detail

Document ID	Billing Charges		MMARS - ITIs	
BCS2023ITD0200POL100	$	186,229.15	$	186,229.15
PAS2023ITD0201POL100	$	3,117.82	$	3,117.82
PAD2023ITD0400POL100	$	199.06	$	199.06
Total:	$	189,546.03	$	189,546.03

Service Detail

		Current Month			Prior Month			YTD		
Code	Description	Units	Rate	Charges	Units	Rate	Charges	Units	Rate	Charges
	Administration									
SL110	TSS Credit Adjustment			$ 0.00	0.00	0.0000	$ 0.00	-1,529.52	1.0000	$ (1,529.52)
	Total Administration:						$ 0.00			$ (1,529.52)
	End User									
SN100	M365 G3	3,289.00	33.8100	$ 111,201.09	3,307.00	33.8100	$ 111,809.67	32,632.00	33.8100	$ 1,103,287.92
SN101	Exchange Online Plan 2	442.00	5.9600	$ 2,634.32	439.00	5.9600	$ 2,616.44	5,976.00	5.9600	$ 35,616.96
SN200	End User Software	3,195.07	1.0000	$ 3,195.07	3,125.77	1.0000	$ 3,125.77	23,136.75	1.0000	$ 23,136.75
SW010	VPN	1,233.00	8.0000	$ 9,864.00	1,226.00	8.0000	$ 9,808.00	11,676.00	8.0000	$ 93,408.00
SW041	Messaging Infrastructure	3,289.00	2.8325	$ 9,307.87	3,307.00	2.8325	$ 9,358.81	32,642.00	2.8325	$ 92,376.86
	Total End User:			$ 136,202.35			$ 136,718.69			$ 1,347,826.49
	Hosting									
SV570	Database Shared Oracle Cluster	1.00	129.7800	$ 129.78	1.00	129.7800	$ 129.78	10.00	129.7800	$ 1,297.80
	Total Hosting:			$ 129.78			$ 129.78			$ 1,297.80
	Mail									
SM191	Document Insertion	2,160.00	0.0579	$ 125.04	2,561.00	0.0579	$ 148.26	30,249.00	0.0579	$ 1,751.12
SM1A1	Metered Mailing	35.40	2.0909	$ 74.02	74.40	2.0909	$ 155.56	666.39	2.0909	$ 1,393.37
	Total Mail:			$ 199.06			$ 303.82			$ 3,144.49
	Pass-Through									
SL000	Vendor Pass-Through	3,117.82	1.0000	$ 3,117.82	8,082.27	1.0000	$ 8,082.27	143,267.74	1.0000	$ 143,267.74
	Total Pass-Through:			$ 3,117.82			$ 8,082.27			$ 143,267.74

		Current Month			Prior Month			YTD		
Code	Description	Units	Rate	Charges	Units	Rate	Charges	Units	Rate	Charges
	Print									
SC111	Printing	3.93	24.7200	$ 97.08	4.68	24.7200	$ 115.67	67.21	24.7200	$ 1,661.42
	Total Print:			$ 97.08			$ 115.67			$ 1,661.42
	Security									
SU080	Digital Certificates			$ 0.00	0.00	0.0000	$ 0.00	1.00	536.6300	$ 536.63
	Total Security:						$ 0.00			$ 536.63
	Unified Communications									
SJ3A0	100Mbps On Network EDI EVC	44.00	900.0000	$ 39,600.00	44.00	900.0000	$ 39,600.00	454.00	900.0000	$ 408,600.00
SJ3A1	200Mbps EDI EVC	2.00	1,250.0000	$ 2,500.00	2.00	1,250.0000	$ 2,500.00	6.00	1,250.0000	$ 7,500.00
SJ3D0	50Mbps ENS	6.00	525.0000	$ 3,150.00	6.00	525.0000	$ 3,150.00	58.00	525.0000	$ 30,450.00
SJ3G0	50Mbps On Network EDI EVC	2.00	650.0000	$ 1,300.00	2.00	650.0000	$ 1,300.00	20.00	650.0000	$ 13,000.00
SJ3J0	100Mbps ENS	2.00	650.0000	$ 1,300.00	2.00	650.0000	$ 1,300.00	20.00	650.0000	$ 13,000.00
SJ6D2	MassIT Connect MagNET 50Mbps	1.00	795.6750	$ 795.68	1.00	795.6750	$ 795.68	10.00	795.6750	$ 7,956.80
SJ6Q2	MassIT Connect MagNET 100Mbps	1.00	1,154.2592	$ 1,154.26	1.00	1,154.2592	$ 1,154.26	10.00	1,154.2592	$ 11,542.60
	Total Unified Communications:			$ 49,799.94			$ 49,799.94			$ 492,049.40
	Grand Total									
	Total:			$ 189,546.03			$ 195,150.17			$ 1,988,254.45

Pass-Through Detail

Task Order	Account Code	EOTSS Doc Identifier	Vendor	Description	Business Item	Charge
003176	POL01050	23040523308000000000	CROWN CASTLE FIBER LLC		Saugus site license (tower & shelter; etc.) renewa	$ 3,090.00
003749	POL01050	23040523308000000000	CROWN CASTLE FIBER LLC		PCR-23-00765 Saugus site license renewal for POL -	$ 27.82
Total:						$ 3,117.82

FY23 December Invoice for POL

Charge Summary

MMARS Code	Description		Amount
BCS	Computer Resources (ChargeBack)	$	186,278.79
PAD	FOR THE PURCHASE & HANDLING OF SUPPLIES	$	580.51
PAS	Tech Services Pass Through	$	40,296.90
Total:		$	227,156.20

Document ID Detail

Document ID	Billing Charges		MMARS - ITIs	
BCS2023ITD0200POL060	$	186,278.79	$	186,278.79
PAS2023ITD0201POL060	$	40,296.90	$	40,296.90
PAD2023ITD0400POL060	$	580.51	$	580.51
Total:	$	227,156.20	$	227,156.20

Service Detail

		Current Month			Prior Month			YTD		
Code	Description	Units	Rate	Charges	Units	Rate	Charges	Units	Rate	Charges
	End User									
SN100	M365 G3	3,310.00	33.8100	$ 111,911.10	3,322.00	33.8100	$ 112,316.82	19,424.00	33.8100	$ 656,725.44
SN101	Exchange Online Plan 2	633.00	5.9600	$ 3,772.68	635.00	5.9600	$ 3,784.60	3,820.00	5.9600	$ 22,767.20
SN200	End User Software	2,391.81	1.0000	$ 2,391.81	2,098.55	1.0000	$ 2,098.55	11,423.89	1.0000	$ 11,423.89
SW010	VPN	1,182.00	8.0000	$ 9,456.00	1,170.00	8.0000	$ 9,360.00	6,822.00	8.0000	$ 54,576.00
SW041	Messaging Infrastructure	3,311.00	2.8325	$ 9,370.13	3,324.00	2.8325	$ 9,406.92	19,433.00	2.8325	$ 54,995.39
	Total End User:			$ 136,901.72			$ 136,966.89			$ 800,487.92
	Hosting									
SV570	Database Shared Oracle Cluster	1.00	129.7800	$ 129.78	1.00	129.7800	$ 129.78	6.00	129.7800	$ 778.68
	Total Hosting:			$ 129.78			$ 129.78			$ 778.68
	Mail									
SM191	Document Insertion	2,431.00	0.0579	$ 140.73	3,392.00	0.0579	$ 196.36	20,408.00	0.0579	$ 1,181.42
SM1A1	Metered Mailing	210.33	2.0909	$ 439.78	33.06	2.0909	$ 69.13	395.46	2.0909	$ 826.88
	Total Mail:			$ 580.51			$ 265.49			$ 2,008.30
	Pass-Through									
SL000	Vendor Pass-Through	40,296.90	1.0000	$ 40,296.90	3,090.00	1.0000	$ 3,090.00	61,337.65	1.0000	$ 61,337.65
	Total Pass-Through:			$ 40,296.90			$ 3,090.00			$ 61,337.65
	Print									
SC111	Printing	5.96	24.7200	$ 147.35	9.53	24.7200	$ 235.66	49.37	24.7200	$ 1,220.28
	Total Print:			$ 147.35			$ 235.66			$ 1,220.28

		Current Month			Prior Month			YTD		
Code	Description	Units	Rate	Charges	Units	Rate	Charges	Units	Rate	Charges
	Unified Communications									
SJ3A0	100Mbps On Network EDI EVC	46.00	900.0000	$ 41,400.00	46.00	900.0000	$ 41,400.00	276.00	900.0000	$ 248,400.00
SJ3D0	50Mbps ENS	6.00	525.0000	$ 3,150.00	6.00	525.0000	$ 3,150.00	34.00	525.0000	$ 17,850.00
SJ3G0	50Mbps On Network EDI EVC	2.00	650.0000	$ 1,300.00	2.00	650.0000	$ 1,300.00	12.00	650.0000	$ 7,800.00
SJ3J0	100Mbps ENS	2.00	650.0000	$ 1,300.00	2.00	650.0000	$ 1,300.00	12.00	650.0000	$ 7,800.00
SJ6D2	MassIT Connect MagNET 50Mbps	1.00	795.6750	$ 795.68	1.00	795.6750	$ 795.68	6.00	795.6750	$ 4,774.08
SJ6Q2	MassIT Connect MagNET 100Mbps	1.00	1,154.2592	$ 1,154.26	1.00	1,154.2592	$ 1,154.26	6.00	1,154.2592	$ 6,925.56
	Total Unified Communications:			$ 49,099.94			$ 49,099.94			$ 293,549.64
	Grand Total									
	Total:			$ 227,156.20			$ 189,787.76			$ 1,159,382.47

Pass-Through Detail

Task Order	Account Code	EOTSS Doc Identifier	Vendor	Description	Business Item	Charge
003176	POL01050	23120122300000000000	CROWN CASTLE FIBER LLC		Saugus site license (tower & shelter; etc.) renewa	$ 3,090.00
003225	POL01050	23122222300000000000	CONVERGEONE; INC		MSP-Body Worn Camera; moves to ConvergeOne	$ 39,165.16
003225	POL01050	23122222300000000000	CONVERGEONE; INC	Prompt payment discount	MSP-Body Worn Camera; moves to ConvergeOne	$ (1,958.26)
Total:						$ 40,296.90

FY23 February Invoice for Department of Police

Charge Summary

MMARS Code	Description		Amount
BCS	Computer Resources (ChargeBack)	$	187,595.32
PAD	FOR THE PURCHASE & HANDLING OF SUPPLIES	$	176.77
PAS	Tech Services Pass Through	$	3,090.00
Total:		$	190,862.09

Document ID Detail

Document ID	Billing Charges		MMARS - ITIs	
BCS2023ITD0200POL080	$	187,595.32	$	187,595.32
PAS2023ITD0201POL080	$	3,090.00	$	3,090.00
PAD2023ITD0400POL080	$	176.77	$	176.77
Total:	$	190,862.09	$	190,862.09

Service Detail

		Current Month			Prior Month			YTD		
Code	Description	Units	Rate	Charges	Units	Rate	Charges	Units	Rate	Charges
	End User									
SN100	M365 G3	3,304.00	33.8100	$ 111,708.24	3,308.00	33.8100	$ 111,843.48	26,036.00	33.8100	$ 880,277.16
SN101	Exchange Online Plan 2	641.00	5.9600	$ 3,820.36	634.00	5.9600	$ 3,778.64	5,095.00	5.9600	$ 30,366.20
SN200	End User Software	2,985.60	1.0000	$ 2,985.60	2,406.42	1.0000	$ 2,406.42	16,815.91	1.0000	$ 16,815.91
SW010	VPN	1,213.00	8.0000	$ 9,704.00	1,182.00	8.0000	$ 9,456.00	9,217.00	8.0000	$ 73,736.00
SW041	Messaging Infrastructure	3,304.00	2.8325	$ 9,350.32	3,309.00	2.8325	$ 9,364.47	26,046.00	2.8325	$ 73,710.18
	Total End User:			$ 137,568.52			$ 136,849.01			$ 1,074,905.45
	Hosting									
SV570	Database Shared Oracle Cluster	1.00	129.7800	$ 129.78	1.00	129.7800	$ 129.78	8.00	129.7800	$ 1,038.24
	Total Hosting:			$ 129.78			$ 129.78			$ 1,038.24
	Mail									
SM191	Document Insertion	1,905.00	0.0579	$ 110.28	3,215.00	0.0579	$ 186.12	25,528.00	0.0579	$ 1,477.82
SM1A1	Metered Mailing	31.80	2.0909	$ 66.49	129.33	2.0909	$ 270.42	556.59	2.0909	$ 1,163.79
	Total Mail:			$ 176.77			$ 456.54			$ 2,641.61
	Pass-Through									
SL000	Vendor Pass-Through	3,090.00	1.0000	$ 3,090.00	67,640.00	1.0000	$ 67,640.00	132,067.65	1.0000	$ 132,067.65
	Total Pass-Through:			$ 3,090.00			$ 67,640.00			$ 132,067.65
	Print									
SC111	Printing	3.93	24.7200	$ 97.08	5.31	24.7200	$ 131.31	58.60	24.7200	$ 1,448.67
	Total Print:			$ 97.08			$ 131.31			$ 1,448.67

		Current Month			Prior Month			YTD		
Code	Description	Units	Rate	Charges	Units	Rate	Charges	Units	Rate	Charges
	Unified Communications									
SJ3A0	100Mbps On Network EDI EVC	44.00	900.0000	$ 39,600.00	46.00	900.0000	$ 41,400.00	366.00	900.0000	$ 329,400.00
SJ3A1	200Mbps EDI EVC	2.00	1,250.0000	$ 2,500.00	0.00	0.0000	$ 0.00	2.00	1,250.0000	$ 2,500.00
SJ3D0	50Mbps ENS	6.00	525.0000	$ 3,150.00	6.00	525.0000	$ 3,150.00	46.00	525.0000	$ 24,150.00
SJ3G0	50Mbps On Network EDI EVC	2.00	650.0000	$ 1,300.00	2.00	650.0000	$ 1,300.00	16.00	650.0000	$ 10,400.00
SJ3J0	100Mbps ENS	2.00	650.0000	$ 1,300.00	2.00	650.0000	$ 1,300.00	16.00	650.0000	$ 10,400.00
SJ6D2	MassIT Connect MagNET 50Mbps	1.00	795.6750	$ 795.68	1.00	795.6750	$ 795.68	8.00	795.6750	$ 6,365.44
SJ6Q2	MassIT Connect MagNET 100Mbps	1.00	1,154.2592	$ 1,154.26	1.00	1,154.2592	$ 1,154.26	8.00	1,154.2592	$ 9,234.08
	Total Unified Communications:			$ 49,799.94			$ 49,099.94			$ 392,449.52
	Grand Total									
	Total:			$ 190,862.09			$ 254,306.58			$ 1,604,551.14

Pass-Through Detail

Task Order	Account Code	EOTSS Doc Identifier	Vendor	Description	Business Item	Charge
003176	POL01050	23020123301000000000	CROWN CASTLE FIBER LLC		Saugus site license (tower & shelter; etc.) renewa	$ 3,090.00
Total:						$ 3,090.00

FY24 August Invoice for

POL - Department of Police

Charge Summary

MMARS Code	Description		Amount
BCS	Computer Resources (ChargeBack)	$	205,742.47
PAS	Tech Services Pass Through	$	3,491.70
Total:		$	209,234.17

Document ID Detail

Document ID	Billing Charges	MMARS - ITIs
BCS2024ITD0200POL020	$ 205,742.47	$ 205,742.47
PAS2024ITD0201POL020	$ 3,491.70	$ 3,491.70
Total:	$ 209,234.17	$ 209,234.17

Service Detail

		Current Month			Prior Month			YTD		
Code	Description	Units	Rate	Charges	Units	Rate	Charges	Units	Rate	Charges
	End User									
SN100	M365 G3	3,464.00	37.4600	$ 129,761.44	3,464.00	37.4600	$ 129,761.44	6,928.00	37.4600	$ 259,522.88
SN101	Exchange Online Plan 2	562.00	5.9600	$ 3,349.52	562.00	5.9600	$ 3,349.52	1,124.00	5.9600	$ 6,699.04
SN200	End User Software	4,009.89	1.0000	$ 4,009.89	3,998.59	1.0000	$ 3,998.59	8,008.48	1.0000	$ 8,008.48
SW010	VPN	1,273.00	8.0000	$ 10,184.00	1,266.00	8.0000	$ 10,128.00	2,539.00	8.0000	$ 20,312.00
SW041	Messaging Infrastructure	3,464.00	2.8325	$ 9,803.12	3,464.00	2.8325	$ 9,803.12	6,928.00	2.8325	$ 19,606.24
	Total End User:			$ 157,107.97			$ 157,040.67			$ 314,148.64
	Hosting									
SV570	Database Shared Oracle Cluster	2.00	129.7800	$ 259.56	2.00	129.7800	$ 259.56	4.00	129.7800	$ 519.12
	Total Hosting:			$ 259.56			$ 259.56			$ 519.12
	Pass-Through									
SL000	Vendor Pass-Through	3,491.70	1.0000	$ 3,491.70	3,491.70	1.0000	$ 3,491.70	6,983.40	1.0000	$ 6,983.40
	Total Pass-Through:			$ 3,491.70			$ 3,491.70			$ 6,983.40
	Unified Communications									
SJ3A0	100Mbps On Network EDI EVC	43.00	900.0000	$ 38,700.00	43.00	900.0000	$ 38,700.00	86.00	900.0000	$ 77,400.00
SJ3D0	50Mbps ENS	5.00	525.0000	$ 2,625.00	5.00	525.0000	$ 2,625.00	10.00	525.0000	$ 5,250.00
SJ3G0	50Mbps On Network EDI EVC	2.00	650.0000	$ 1,300.00	2.00	650.0000	$ 1,300.00	4.00	650.0000	$ 2,600.00
SJ3H0	100Mbps Off Network EDI EVC	2.00	1,250.0000	$ 2,500.00	2.00	1,250.0000	$ 2,500.00	4.00	1,250.0000	$ 5,000.00
SJ3J0	100Mbps ENS	2.00	650.0000	$ 1,300.00	2.00	650.0000	$ 1,300.00	4.00	650.0000	$ 2,600.00

		Current Month			Prior Month			YTD		
Code	Description	Units	Rate	Charges	Units	Rate	Charges	Units	Rate	Charges
SJ6D2	MassIT Connect MagNET 50Mbps	1.00	795.6750	$ 795.68	1.00	795.6750	$ 795.68	2.00	795.6750	$ 1,591.36
SJ6Q2	MassIT Connect MagNET 100Mbps	1.00	1,154.2592	$ 1,154.26	1.00	1,154.2592	$ 1,154.26	2.00	1,154.2592	$ 2,308.52
	Total Unified Communications:			$ 48,374.94			$ 48,374.94			$ 96,749.88
	Grand Total									
	Total:			$ 209,234.17			$ 209,166.87			$ 418,401.04

Pass-Through Detail

Task Order	Account Code	EOTSS Doc Identifier	Vendor	Description	Business Item	Charge
003749	POL01050	24073123300000000000	CROWN CASTLE FIBER LLC		PCR-23-00765 Saugus site license renewal for POL -	$ 3,491.70
Total:						$ 3,491.70

EXECUTIVE OFFICE OF TECHNOLOGY SERVICES & SECURITY

COMMONWEALTH OF MASSACHUSETTS | 1 ASHBURTON PLACE, 8TH FLOOR, BOSTON, MA 02108

BAR Statement - POL Summary

Warehouse Updated May 26, 2023

FY23 Pass-Through Statement

Billed Through April 2023

					Committed Detail		Expensed Detail			
BAR Date	Task Order	Description	BAR Amount	Committed	Encumbered	Expensed	Pending	Billed	Status	Appropriation
2022-02-15	003098	POL - FY23 - Desktop Modernization Bundle 2 (REQ0183480)	$ 1,529.52	$ 1,529.52	$ 0.00	$ 1,529.52	$ 0.00	$ 1,529.52	Closed	8100-1001
2022-04-01	003176	MSP - FY22 - License Renewal - Crown Castle Monthly Costs for Communications Tower at 57 Cheever Street Saugus - 5/1/22 through 4/20/23	$ 30,900.00	$ 30,900.00	$ 0.00	$ 30,900.00	$ 0.00	$ 30,900.00	Closed	8100-1001
2022-06-01	003258	MSP - MSP Leverett Circle H-4 Network (REQ0203006)	$ 25,784.80	$ 25,784.80	$ 25,784.80	$ 0.00	$ 0.00	$ 0.00	Delinquent	8100-1001
2022-06-01	003282	POL - MSP Body Worn Camera Expansion Project 5 Sites Hardware and Config (REQ0199449)	$ 61,918.79	$ 0.00	$ 0.00	$ 0.00	$ 0.00	$ 0.00	Pending	EOTSS 1790-0201 / POL:: 8100-1001

EXECUTIVE OFFICE OF TECHNOLOGY SERVICES & SECURITY

COMMONWEALTH OF MASSACHUSETTS | 1 ASHBURTON PLACE, 8TH FLOOR, BOSTON, MA 02108

					Committed Detail		Expensed Detail			
BAR Date	Task Order	Description	BAR Amount	Committed	Encumbered	Expensed	Pending	Billed	Status	Appropriation
2022-09-02	003229	POL - Revised - FY22 - Modify Wifi - Additional Access Points - State Police Training Academy, 340 West Brookfield Road, New Braintree (REQ0190977)	$ 5,885.00	$ 5,590.75	$ 0.00	$ 5,590.75	$ 0.00	$ 5,590.75	Closed	8100-1001
2022-09-02	003380	MSP - FY23 - Comcast Circuit Charges (REQ0212659)	$ 569,375.16	$ 0.00	$ 0.00	$ 0.00	$ 0.00	$ 0.00	Pending	8100-1001
2022-09-15	003436	MSP - FY23 - New Switches for Mass State Police Norwell (REQ0217069)	$ 15,108.40	$ 15,108.40	$ 15,108.40	$ 0.00	$ 0.00	$ 0.00	Delinquent	8100-1001
2022-09-15	003443	MSP - FY23 - New Switches for Mass State Police at 2289 Main Street, Athol (REQ0218222)	$ 8,405.20	$ 8,405.20	$ 8,405.20	$ 0.00	$ 0.00	$ 0.00	Delinquent	8100-1001
2022-09-16	003434	OAT - FY23 - Switch Expansion at the Maynard Crime Lab (REQ0214052)	$ 16,384.20	$ 16,201.95	$ 12,739.20	$ 3,462.75	$ 0.00	$ 3,462.75	Open	8100-1004
2022-09-29	003435	POL - New Circuit for Leverett Boston Barracks, 250 Leverett Circle, Boston 50 Mbps (REQ0220144)	$ 6,625.58	$ 0.00	$ 0.00	$ 0.00	$ 0.00	$ 0.00	Pending	8100-1001
2022-10-31	003524	POL - New Comcast ENS Circuit for 35 Braintree Hill Office Park, Braintree 50 Mbps (REQ0224864)	$ 5,900.51	$ 0.00	$ 0.00	$ 0.00	$ 0.00	$ 0.00	Pending	8100-1001

EXECUTIVE OFFICE OF TECHNOLOGY SERVICES & SECURITY

COMMONWEALTH OF MASSACHUSETTS | 1 ASHBURTON PLACE, 8TH FLOOR, BOSTON, MA 02108

				Committed Detail		Expensed Detail			
BAR Date	Task Order	Description	BAR Amount	Committed	Encumbered	Expensed	Pending	Billed	Status	Appropriation
2022-11-15	003544	POL - FY23 - Comcast Temporary Internet Circuit for 35 Braintree Hill Office Park, Braintree 100 Mbps (REQ0224864)	$ 506.65	$ 0.00	$ 0.00	$ 0.00	$ 0.00	$ 0.00	Pending	8100-1001
2022-11-15	003550	POL - FY23 - New Servers - PowerEdge R750 (REQ0229404)	$ 60,050.00	$ 60,050.00	$ 0.00	$ 60,050.00	$ 0.00	$ 60,050.00	Closed	8100-1001
2022-11-30	003562	MSP - FY23 - Crown Castle to install a helicopter Receiver at 57 Cheever Street, Saugus	$ 9,500.00	$ 9,500.00	$ 0.00	$ 9,500.00	$ 5,000.00	$ 4,500.00	Open	
2023-03-14	003739	POL - FY 23 - Request for Desktop hardware at 470 WORCESTER ROAD, Framingham - Special Request - REQ0246082	$ 21,178.74	$ 21,178.74	$ 21,178.74	$ 0.00	$ 0.00	$ 0.00	Delinquent	8100-1001
2023-03-14	003749	MSP - FY23 - License Renewal - Crown Castle Monthly Costs for Communications Tower at 57 Cheever Street Saugus - 4/1/23 - 6/30/24	$ 10,448.10	$ 10,448.10	$ 9,126.08	$ 1,322.02	$ 1,294.20	$ 27.82	Open	8100-1001
2023-04-20	003778	POL - FY23 - Disconnect Circuit at 35 Braintree Hill Office Park, Suite 302 Braintree - 100 Mbps (REQ0251653)	$ (203.35)	$ 0.00	$ 0.00	$ 0.00	$ 0.00	$ 0.00	Pending	
2023-05-01	003802	POL – FY23 - Hardware Special Request HP Zbook (REQ0250916) PAS 0201	$ 6,357.36	$ 6,357.36	$ 6,357.36	$ 0.00	$ 0.00	$ 0.00	Delinquent	8100-1001

EXECUTIVE OFFICE OF TECHNOLOGY SERVICES & SECURITY

COMMONWEALTH OF MASSACHUSETTS | 1 ASHBURTON PLACE, 8TH FLOOR, BOSTON, MA 02108

					Committed Detail		Expensed Detail			
BAR Date	Task Order	Description	BAR Amount	Committed	Encumbered	Expensed	Pending	Billed	Status	Appropriation
2023-05-25	003225	REVISED - POL - Body Worn Camera - MSP Body Worn Camera Expansion Project 8 Sites Config Only (REQ0199449)	$ 77,940.16	$ 83,031.90	$ 45,825.00	$ 37,206.90	$ 0.00	$ 37,206.90	Open	EOTSS 1790-0201 / POL:: 8100-1001
	002984	POL - New MBI - Connect MagNET Circuit at 18 Jacobs Road, Heath - 50 Mbps for (REQ0175382) BCS	$ 10,248.29	$ 0.00	$ 0.00	$ 0.00	$ 0.00	$ 0.00	Pending	8100-1001
Total:			$ 943,843.11	$ 294,086.72	$ 144,524.78	$ 149,561.94	$ 6,294.20	$ 143,267.74		

EXECUTIVE OFFICE OF TECHNOLOGY SERVICES & SECURITY

COMMONWEALTH OF MASSACHUSETTS | 1 ASHBURTON PLACE, 8TH FLOOR, BOSTON, MA 02108

BAR Statement - POL Summary

Warehouse Updated January 26, 2023

FY23 Pass-Through Statement

Billed Through December 2022

					Committed Detail		Expensed Detail			
BAR Date	Task Order	Description	BAR Amount	Committed	Encumbered	Expensed	Pending	Billed	Status	Appropriation
2022-02-15	003098	POL - FY23 - Desktop Modernization Bundle 2 (REQ0183480)	$ 1,529.52	$ 1,529.52	$ 1,529.52	$ 0.00	$ 0.00	$ 0.00	Open	8100-1001
2022-06-01	003225	POL - Body Worn Camera - MSP Body Worn Camera Expansion Project 8 Sites Config Only (REQ0199449)	$ 84,990.16	$ 83,031.90	$ 45,825.00	$ 37,206.90	$ 0.00	$ 37,206.90	Open	EOTSS 1790-0201 / POL:: 8100-1001
2022-06-01	003258	MSP - MSP Leverett Circle H-4 Network (REQ0203006)	$ 25,784.80	$ 25,784.80	$ 25,784.80	$ 0.00	$ 0.00	$ 0.00	Open	8100-1001
2022-06-01	003282	POL - MSP Body Worn Camera Expansion Project 5 Sites Hardware and Config (REQ0199449)	$ 61,918.79	$ 0.00	$ 0.00	$ 0.00	$ 0.00	$ 0.00	Open	EOTSS 1790-0201 / POL:: 8100-1001
2022-09-02	003380	MSP - FY23 - Comcast Circuit Charges (REQ0212659)	$ 569,375.16	$ 0.00	$ 0.00	$ 0.00	$ 0.00	$ 0.00	Open	8100-1001

EXECUTIVE OFFICE OF TECHNOLOGY SERVICES & SECURITY

COMMONWEALTH OF MASSACHUSETTS | 1 ASHBURTON PLACE, 8TH FLOOR, BOSTON, MA 02108

				Committed Detail		Expensed Detail			
BAR Date	Task Order	Description	BAR Amount	Committed	Encumbered	Expensed	Pending	Billed	Status	Appropriation
2022-09-15	003436	MSP - FY23 - New Switches for Mass State Police Norwell (REQ0217069)	$ 15,108.40	$ 15,108.40	$ 15,108.40	$ 0.00	$ 0.00	$ 0.00	Open	8100-1001
2022-09-15	003443	MSP - FY23 - New Switches for Mass State Police at 2289 Main Street, Athol (REQ0218222)	$ 8,405.20	$ 8,405.20	$ 8,405.20	$ 0.00	$ 0.00	$ 0.00	Open	8100-1001
2022-09-16	003434	OAT - FY23 - Switch Expansion at the Maynard Crime Lab (REQ0214052)	$ 16,384.20	$ 16,384.20	$ 16,384.20	$ 0.00	$ 0.00	$ 0.00	Open	8100-1004
2022-09-29	003435	POL - New Circuit for Leverett Boston Barracks, 250 Leverett Circle, Boston 50 Mbps (REQ0220144)	$ 6,625.58	$ 0.00	$ 0.00	$ 0.00	$ 0.00	$ 0.00	Open	8100-1001
2022-10-31	003524	POL - New Comcast ENS Circuit for 35 Braintree Hill Office Park, Braintree 50 Mbps (REQ0224864)	$ 5,900.51	$ 0.00	$ 0.00	$ 0.00	$ 0.00	$ 0.00	Open	8100-1001
2022-11-15	003544	POL - FY23 - Comcast Temporary Internet Circuit for 35 Braintree Hill Office Park, Braintree 100 Mbps (REQ0224864)	$ 506.65	$ 0.00	$ 0.00	$ 0.00	$ 0.00	$ 0.00	Open	8100-1001
2022-11-15	003550	POL - FY23 - New Servers - PowerEdge R750 (REQ0229404)	$ 60,050.00	$ 60,050.00	$ 0.00	$ 60,050.00	$ 60,050.00	$ 0.00	Open	8100-1001
2022-11-30	003562	MSP - FY23 - Crown Castle to install a helicopter Receiver at 57 Cheever Street, Saugus	$ 9,500.00	$ 9,500.00	$ 5,000.00	$ 4,500.00	$ 4,500.00	$ 0.00	Open	

EXECUTIVE OFFICE OF TECHNOLOGY SERVICES & SECURITY

COMMONWEALTH OF MASSACHUSETTS | 1 ASHBURTON PLACE, 8TH FLOOR, BOSTON, MA 02108

					Committed Detail		Expensed Detail			
BAR Date	Task Order	Description	BAR Amount	Committed	Encumbered	Expensed	Pending	Billed	Status	Appropriation
	003176		$ 30,900.00	$ 30,900.00	$ 12,360.00	$ 18,540.00	$ 0.00	$ 18,540.00	Open	
	003229		$ 5,590.75	$ 5,590.75	$ 0.00	$ 5,590.75	$ 0.00	$ 5,590.75	Closed	
Total:			$ 902,569.72	$ 256,284.77	$ 130,397.12	$ 125,887.65	$ 64,550.00	$ 61,337.65		

EXECUTIVE OFFICE OF TECHNOLOGY SERVICES & SECURITY

COMMONWEALTH OF MASSACHUSETTS | 1 ASHBURTON PLACE, 8TH FLOOR, BOSTON, MA 02108

BAR Statement - POL Summary

Warehouse Updated April 12, 2023

FY23 Pass-Through Statement

Billed Through February 2023

				Committed Detail		Expensed Detail			
BAR Date	Task Order	Description	BAR Amount	Committed	Encumbered	Expensed	Pending	Billed	Status	Appropriation
2022-02-15	003098	POL - FY23 - Desktop Modernization Bundle 2 (REQ0183480)	$ 1,529.52	$ 1,529.52	$ 0.00	$ 1,529.52	$ 1,529.52	$ 0.00	Open	8100-1001
2022-06-01	003225	POL - Body Worn Camera - MSP Body Worn Camera Expansion Project 8 Sites Config Only (REQ0199449)	$ 84,990.16	$ 83,031.90	$ 45,825.00	$ 37,206.90	$ 0.00	$ 37,206.90	Open	EOTSS 1790-0201 / POL:: 8100-1001
2022-06-01	003258	MSP - MSP Leverett Circle H-4 Network (REQ0203006)	$ 25,784.80	$ 25,784.80	$ 25,784.80	$ 0.00	$ 0.00	$ 0.00	Open	8100-1001
2022-06-01	003282	POL - MSP Body Worn Camera Expansion Project 5 Sites Hardware and Config (REQ0199449)	$ 61,918.79	$ 0.00	$ 0.00	$ 0.00	$ 0.00	$ 0.00	Open	EOTSS 1790-0201 / POL:: 8100-1001
2022-09-02	003380	MSP - FY23 - Comcast Circuit Charges (REQ0212659)	$ 569,375.16	$ 0.00	$ 0.00	$ 0.00	$ 0.00	$ 0.00	Open	8100-1001

EXECUTIVE OFFICE OF TECHNOLOGY SERVICES & SECURITY

COMMONWEALTH OF MASSACHUSETTS | 1 ASHBURTON PLACE, 8TH FLOOR, BOSTON, MA 02108

				Committed Detail		Expensed Detail			
BAR Date	Task Order	Description	BAR Amount	Committed	Encumbered	Expensed	Pending	Billed	Status	Appropriation
2022-09-15	003436	MSP - FY23 - New Switches for Mass State Police Norwell (REQ0217069)	$ 15,108.40	$ 15,108.40	$ 15,108.40	$ 0.00	$ 0.00	$ 0.00	Open	8100-1001
2022-09-15	003443	MSP - FY23 - New Switches for Mass State Police at 2289 Main Street, Athol (REQ0218222)	$ 8,405.20	$ 8,405.20	$ 8,405.20	$ 0.00	$ 0.00	$ 0.00	Open	8100-1001
2022-09-16	003434	OAT - FY23 - Switch Expansion at the Maynard Crime Lab (REQ0214052)	$ 16,384.20	$ 16,201.95	$ 12,739.20	$ 3,462.75	$ 3,462.75	$ 0.00	Open	8100-1004
2022-09-29	003435	POL - New Circuit for Leverett Boston Barracks, 250 Leverett Circle, Boston 50 Mbps (REQ0220144)	$ 6,625.58	$ 0.00	$ 0.00	$ 0.00	$ 0.00	$ 0.00	Open	8100-1001
2022-10-31	003524	POL - New Comcast ENS Circuit for 35 Braintree Hill Office Park, Braintree 50 Mbps (REQ0224864)	$ 5,900.51	$ 0.00	$ 0.00	$ 0.00	$ 0.00	$ 0.00	Open	8100-1001
2022-11-15	003544	POL - FY23 - Comcast Temporary Internet Circuit for 35 Braintree Hill Office Park, Braintree 100 Mbps (REQ0224864)	$ 506.65	$ 0.00	$ 0.00	$ 0.00	$ 0.00	$ 0.00	Open	8100-1001
2022-11-15	003550	POL - FY23 - New Servers - PowerEdge R750 (REQ0229404)	$ 60,050.00	$ 60,050.00	$ 0.00	$ 60,050.00	$ 0.00	$ 60,050.00	Closed	8100-1001
2022-11-30	003562	MSP - FY23 - Crown Castle to install a helicopter Receiver at 57 Cheever Street, Saugus	$ 9,500.00	$ 9,500.00	$ 5,000.00	$ 4,500.00	$ 0.00	$ 4,500.00	Open	

EXECUTIVE OFFICE OF TECHNOLOGY SERVICES & SECURITY

COMMONWEALTH OF MASSACHUSETTS | 1 ASHBURTON PLACE, 8TH FLOOR, BOSTON, MA 02108

					Committed Detail		Expensed Detail			
BAR Date	Task Order	Description	BAR Amount	Committed	Encumbered	Expensed	Pending	Billed	Status	Appropriation
2023-03-14	003739	POL - FY 23 - Request for Desktop hardware at 470 WORCESTER ROAD, Framingham - Special Request - REQ0246082	$ 21,178.74	$ 21,178.74	$ 21,178.74	$ 0.00	$ 0.00	$ 0.00	Open	8100-1001
2023-03-14	003749	MSP - FY23 - License Renewal - Crown Castle Monthly Costs for Communications Tower at 57 Cheever Street Saugus - 4/1/23 - 6/30/24	$ 10,448.10	$ 10,448.10	$ 10,448.10	$ 0.00	$ 0.00	$ 0.00	Open	8100-1001
	003176		$ 30,900.00	$ 30,900.00	$ 3,090.00	$ 27,810.00	$ 3,090.00	$ 24,720.00	Open	
	003229		$ 5,590.75	$ 5,590.75	$ 0.00	$ 5,590.75	$ 0.00	$ 5,590.75	Closed	
	003778	POL - FY23 - Disconnect Circuit at 35 Braintree Hill Office Park, Suite 302 Braintree - 100 Mbps (REQ0251653)	$ (203.35)	$ 0.00	$ 0.00	$ 0.00	$ 0.00	$ 0.00	Open	
Total:			$ 933,993.21	$ 287,729.36	$ 147,579.44	$ 140,149.92	$ 8,082.27	$ 132,067.65		

EXECUTIVE OFFICE OF TECHNOLOGY SERVICES & SECURITY

COMMONWEALTH OF MASSACHUSETTS | 1 ASHBURTON PLACE, 8TH FLOOR, BOSTON, MA 02108

FY24 Pass-Through Statement

POL - Department of Police

Warehouse Updated October 19, 2023

Billed Through August 2023

Active BARs

BAR Date	Task Order	Account Code	Description	BAR Amount	Committed Detail		Expensed Detail		Status	Customer Appropriation
					Committed	Encumbered and Accrued	Cash Expensed	Pending	Billed		
2023-09-14	003966	POL01050	MSP - FY24 - Comcast Circuit Charges (REQ0272650) PAS0201	$ 637,775.16	$ 0.00	$ 0.00	$ 0.00	$ 0.00	$ 0.00	Open	8100-1001
2023-08-14	003942	POL01050	POL - FY24 - Modify Wireless - MSP Aruba Wireless + Cabling - Northampton, Millbury and South Boston(REQ0270186) PAS0201	$ 8,342.92	$ 8,342.92	$ 8,342.92	$ 0.00	$ 0.00	$ 0.00	Open	8100-4443
2023-05-25	003225	POL01050	REVISED - POL - Body Worn Camera - MSP Body Worn Camera Expansion Project 8 Sites Config Only (REQ0199449)	$ 7,050.00	$ 7,050.00	$ 7,050.00	$ 0.00	$ 0.00	$ 0.00	Open	EOTSS 1790-0201 / POL:: 8100-1001
2023-04-25	003801	POL01050	MSP - FY24 - Routers and Switches for MassVoice – Voice over Internet Protocol (VOIP) on Command Post 1 (CP1) Vehicle (REQ0254245) PAS 0201	$ 85,340.80	$ 85,340.80	$ 85,340.80	$ 0.00	$ 0.00	$ 0.00	Open	8100-4443
2023-04-20	003779	POL01050	POL - FY 24 - New Wifi - MSP H4 250 Leverett Circle Boston - REQ0236023	$ 28,627.42	$ 28,627.42	$ 28,627.42	$ 0.00	$ 0.00	$ 0.00	Open	8100-1001

EXECUTIVE OFFICE OF TECHNOLOGY SERVICES & SECURITY

COMMONWEALTH OF MASSACHUSETTS | 1 ASHBURTON PLACE, 8TH FLOOR, BOSTON, MA 02108

BAR Date	Task Order	Account Code	Description	BAR Amount	Committed	Committed Detail: Encumbered and Accrued	Committed Detail: Cash Expensed	Expensed Detail: Pending	Expensed Detail: Billed	Status	Customer Appropriation
2023-03-14	003749	POL01050	MSP - FY23 - License Renewal - Crown Castle Monthly Costs for Communications Tower at 57 Cheever Street Saugus - 4/1/23 - 6/30/24	$ 42,105.84	$ 35,088.20	$ 24,613.10	$ 10,475.10	$ 0.00	$ 10,475.10	Open	8100-1001
2022-10-31	003524	POL01050	POL - New Comcast ENS Circuit for 35 Braintree Hill Office Park, Braintree 50 Mbps (REQ0224864)	$ 8,700.84	$ 0.00	$ 0.00	$ 0.00	$ 0.00	$ 0.00	Open	8100-1001
2022-09-29	003435	POL01050	POL - New Circuit for Leverett Boston Barracks, 250 Leverett Circle, Boston 50 Mbps (REQ0220144)	$ 8,700.84	$ 0.00	$ 0.00	$ 0.00	$ 0.00	$ 0.00	Open	8100-1001
Totals for 8 Active BARs:				$ 826,643.82	$ 164,449.34	$ 153,974.24	$ 10,475.10	$ 0.00	$ 10,475.10		

Your current active BARs total $826,643.82

Your IE in MMARS (PAS2024ITD0201POL000) is currently set at $0.00

EXECUTIVE OFFICE OF TECHNOLOGY SERVICES & SECURITY

COMMONWEALTH OF MASSACHUSETTS | 1 ASHBURTON PLACE, 8TH FLOOR, BOSTON, MA 02108

Canceled BARs

BAR Date	Task Order	Account Code	Description	BAR Amount	Committed	Committed Detail		Expensed Detail		Status	Customer Appropriation
						Encumbered and Accrued	Cash Expensed	Pending	Billed		
Totals for 0 Canceled BARs:											

3054



ELSAG
Automatic License Plate Recognition (ALPR) Technology Briefing

LEONARDO

ELSAG
Advancing License Plate Recognition

A division of and with the resources of Leonardo, a US$13 Billion global leader in Defense, Security, Law Enforcement and National Security, to develop long term solutions for your public safety needs.



EOC
ENTERPRISE OPERATIONS CENTER



© Selex ES Inc., a Leonardo Company

The Benefits of ALPL

Supporting Police Work

- ❖ Recovery of stolen vehicles
- ❖ Motorway monitoring
- ❖ Disrupting major crime and Terrorism
- ❖ Surveillance
- ❖ Border control
- ❖ Homeland Security initiatives

EOC
ENTERPRISE OPERATIONS CENTER

Criminal Intelligence

Target profiling

Crime Scene Investigations

Criminal Pattern Analysis

Critical Infrastructure

Watch-list Development

Terrorist Interdiction

Managing Today's Work → Preventing Tomorrow's Threat

Advantages of ELSAG Quality

Hardware :

• 100% immersion of cameras during manufacturing in 1 meter water

• 100% testing in hot/cold chamber from room temp to +60C to -40C

• 100% camera final seal in nitrogen vacuum for weatherproof performance

• Advanced Digital Progressive Scan HD cameras (not analogue) for highest accuracy

• Technology started with Mobile then progressed to Fixed; most advanced in speed, capture rate, viewing angle and real time transmission in ALPR/ANPR industry

Software :

• Industry leading OCR Optical Character Recognition Algorithms

• Web based XMPP real time meta data for fastest analytic results

• OCR Protocols started with USA Plates

(with multiple characters, artwork, anomalies)

resulting in most flexible, robust OCR in industry.



© Selex ES Inc., a Leonardo Company

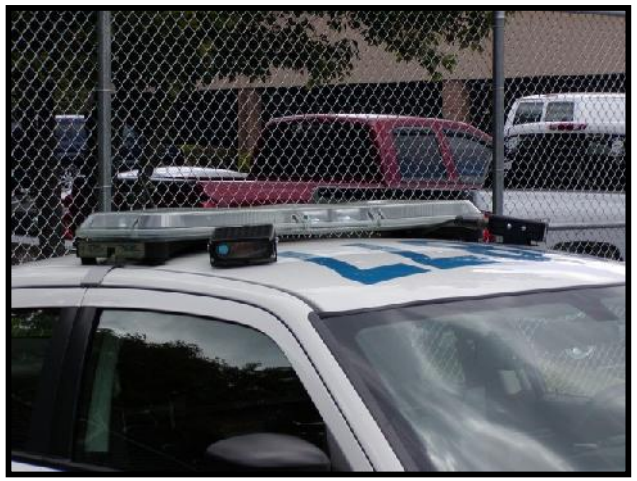
ELSAG's Mobile ALPR Deployments













MPH
Mobile Plate Hunter

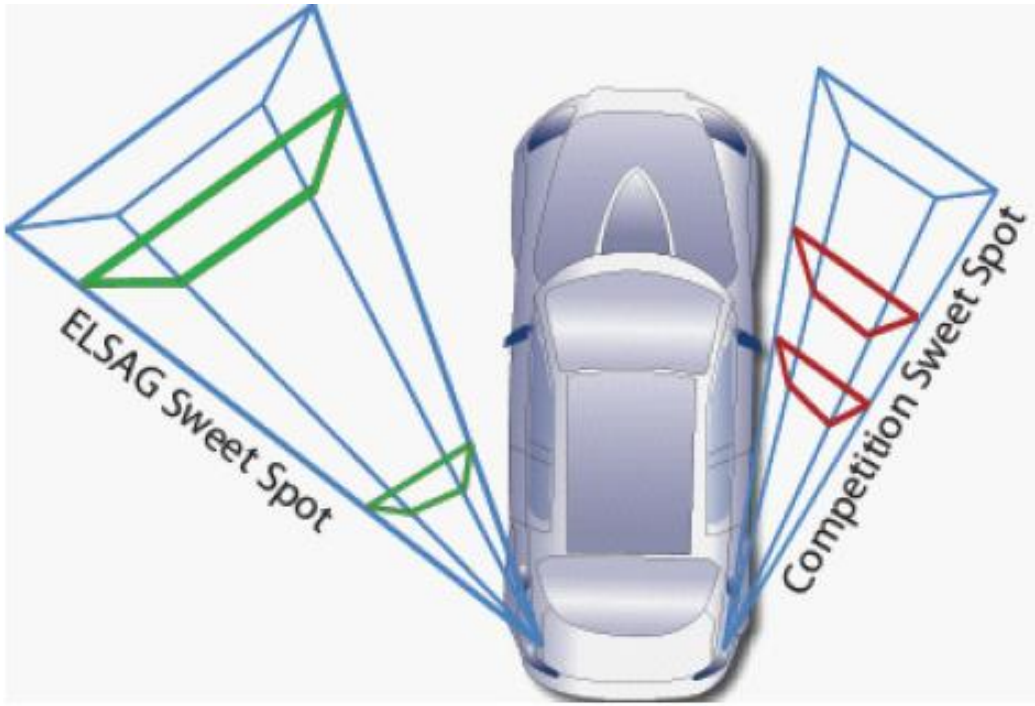
- A Mobile ALPR system capturing over 900 reads per minute (15/sec)
- Captures vehicles in excess of 150 MPH / 250 KPH closing speeds.
- MPH-900 requires no driver intervention and runs against over 4.0 million lines of hot-list files for vehicles of interest.
- Milliseconds after a Hot list vehicle is captured, the system sounds an audible & visual alarm to the operator for immediate response.
- MPH-900 reads plates from all countries including difficult to read flat and vanity tags – 24 hours DAY or NIGHT in all kinds of weather.

MPH900
Mobile Plate Hunter 900 Series



© Selex ES Inc., a Leonardo Company

ELSAG's Viewing Range vs The Competition



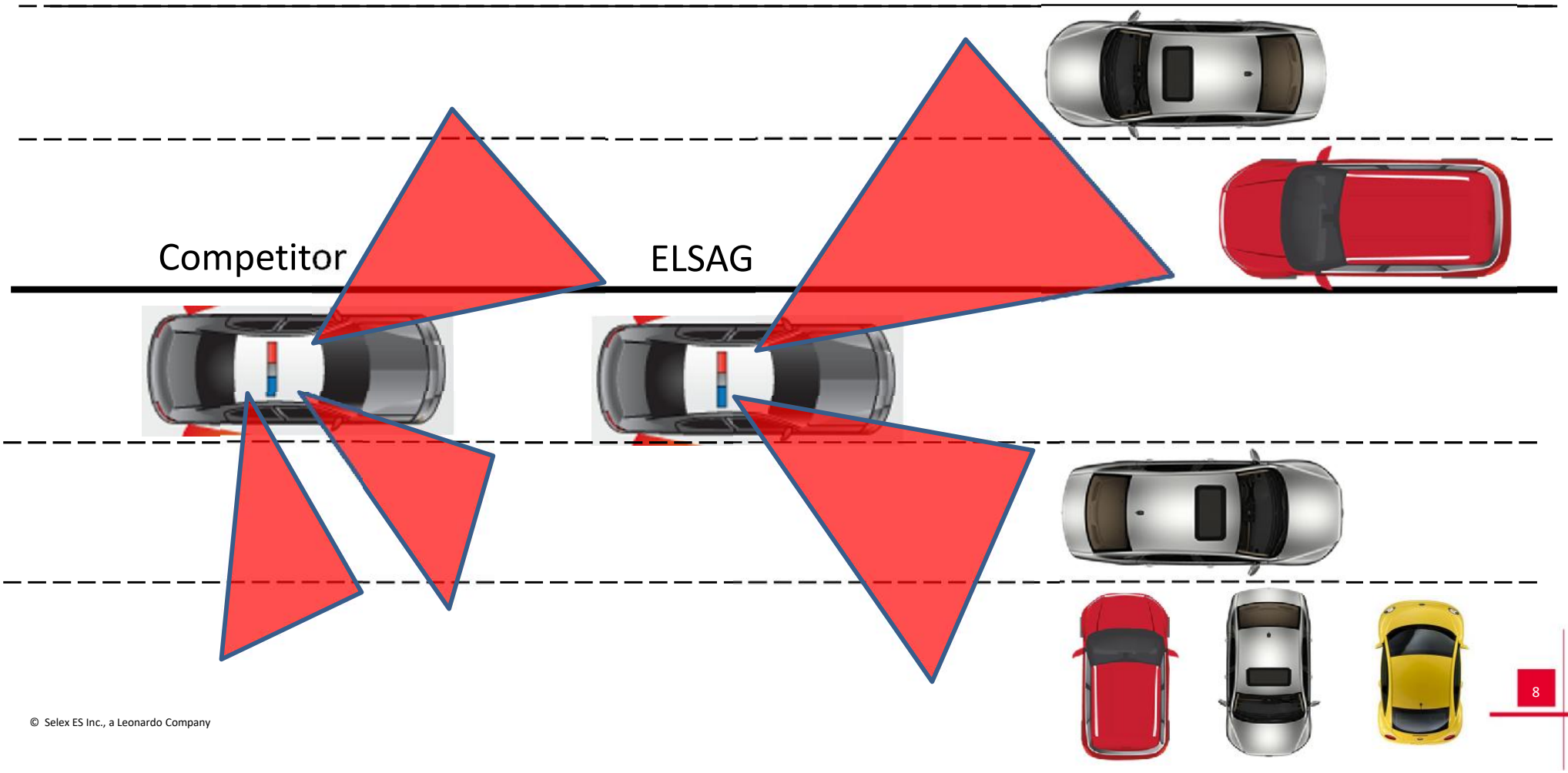


- ELSAG's Viewing Range is nearly twice the size of the other LPR systems
- ELSAG's Digital High Resolution (1280 x 1024) Cameras read plates with wider and higher viewing ranges than the other LPR systems
- ELSAG's Larger Viewing Range helps to identify more of the vehicle on color photos and capture more plates !

© Selex ES Inc., a Leonardo Company

Elsag MPH M7 Aiming Scenario : 16mm camera on Drivers Side; 12mm on Passenger side Wider viewing cameras capture cars in parallel lane and also 90 degree parked angles

Competitor Aiming Scenario : 3 cameras are needed since Passenger side camera viewing range is less wide, 1 camera is required to capture cars in parallel lane and an additional camera is needed for 90 degree parked angles



© Selex ES Inc., a Leonardo Company

ELSAG's Fixed ALPR Deployments













Covert Camera



ELSAG's Covert Plate Hunter Solutions



Ladder Camera



Engine Cameras



Rooftop Carrier



Traffic Covert barrel camera





Covert Pole Mount with appearance of electrical box



Under-Cover Police ANPR in Taxi advertising light box



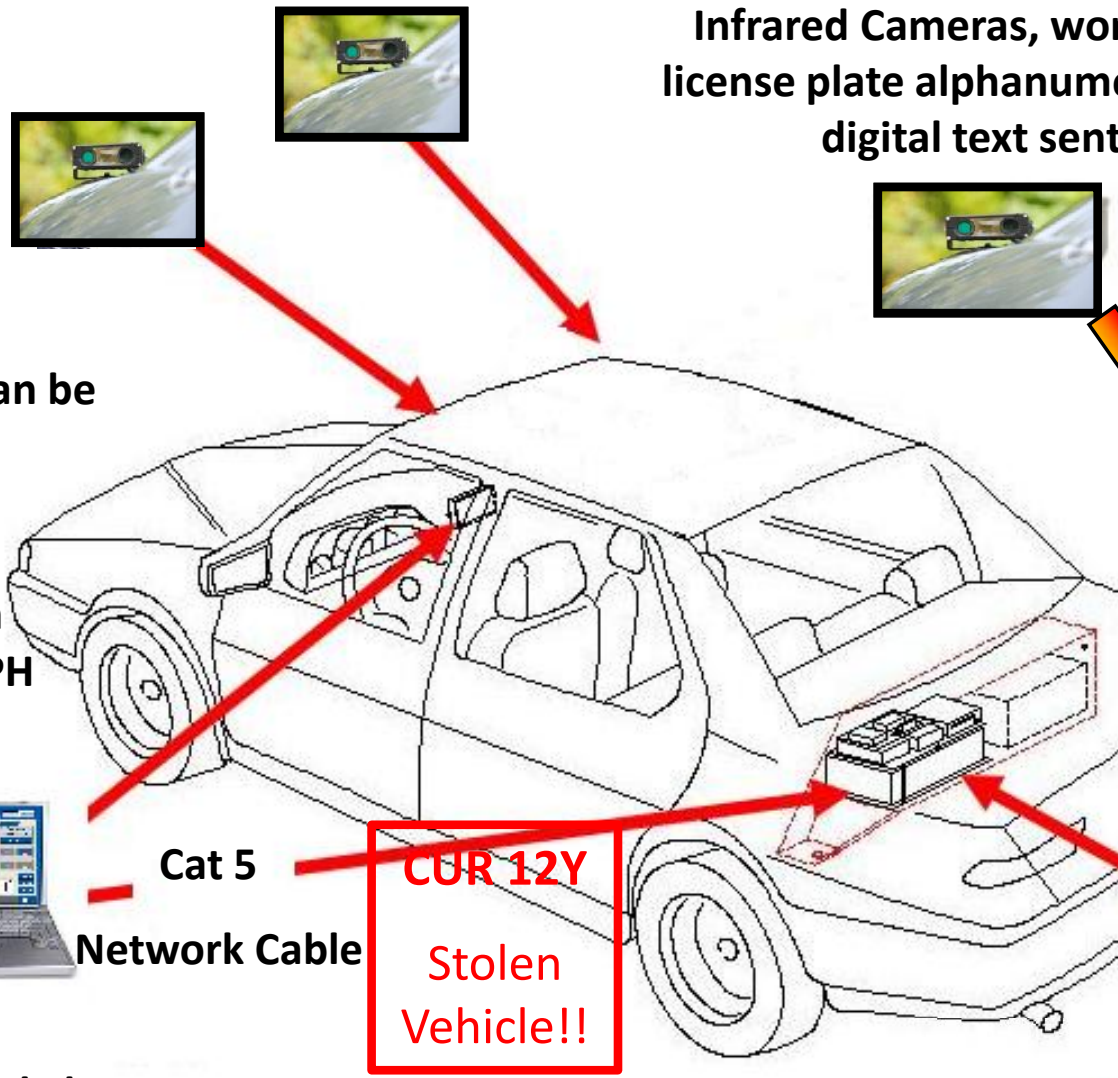
Push Bumper

How ALPR Works

Infrared Cameras, work day or night to capture license plate alphanumeric string and convert into digital text sent to OCR processor.



Number plates can be read anywhere in the camera's field of view at Closing speeds in excess of 150 MPH



CUR 12Y

Cat 5

Network Cable

CUR 12Y

Stolen Vehicle!!

Audible and visual alarms notify the officer that intervention is necessary

© Selex ES Inc., a Leonardo Company

Supporting ALPR/ANPR Mission 24/7

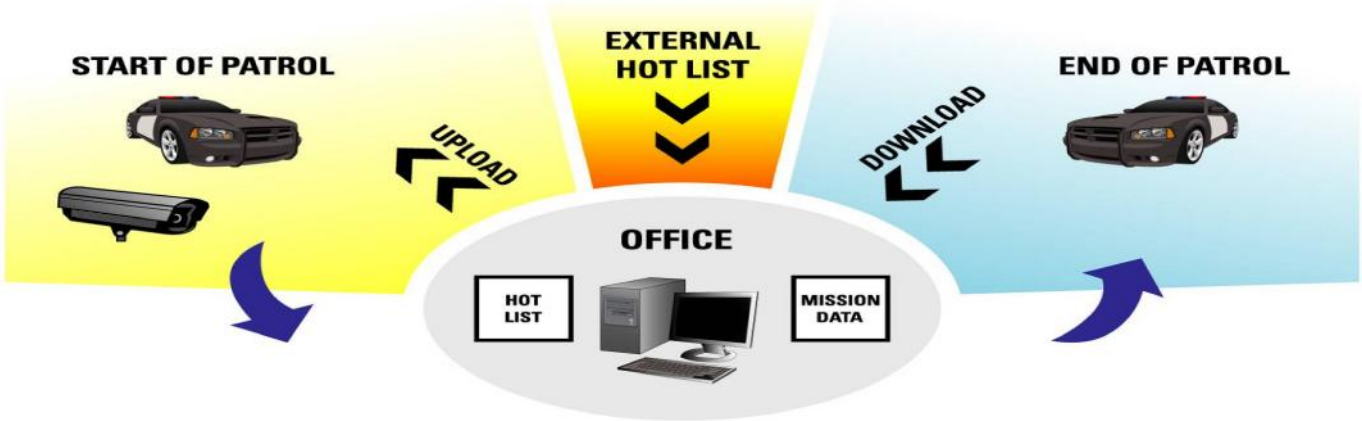
GOOD POLICE WORK

Stolen Vehicles
Stolen Plates
Wants & Warrants
Gang & Terrorist Watchlists
Suspended Plates
ScoffLaws

MPH900 Mobile Plate Hunter 900 by Selex
REMINGTON ELSAG LAW ENFORCEMENT SYSTEMS
Command Center Software Suite

CRIMINAL INTELLIGENCE

After Action Analytics
Crime Scene Investigations
Criminal Pattern Analytics
Critical Infrastructure
Watchlist Development
Terrorist Interdiction





© Selex ES Inc., a Leonardo Company

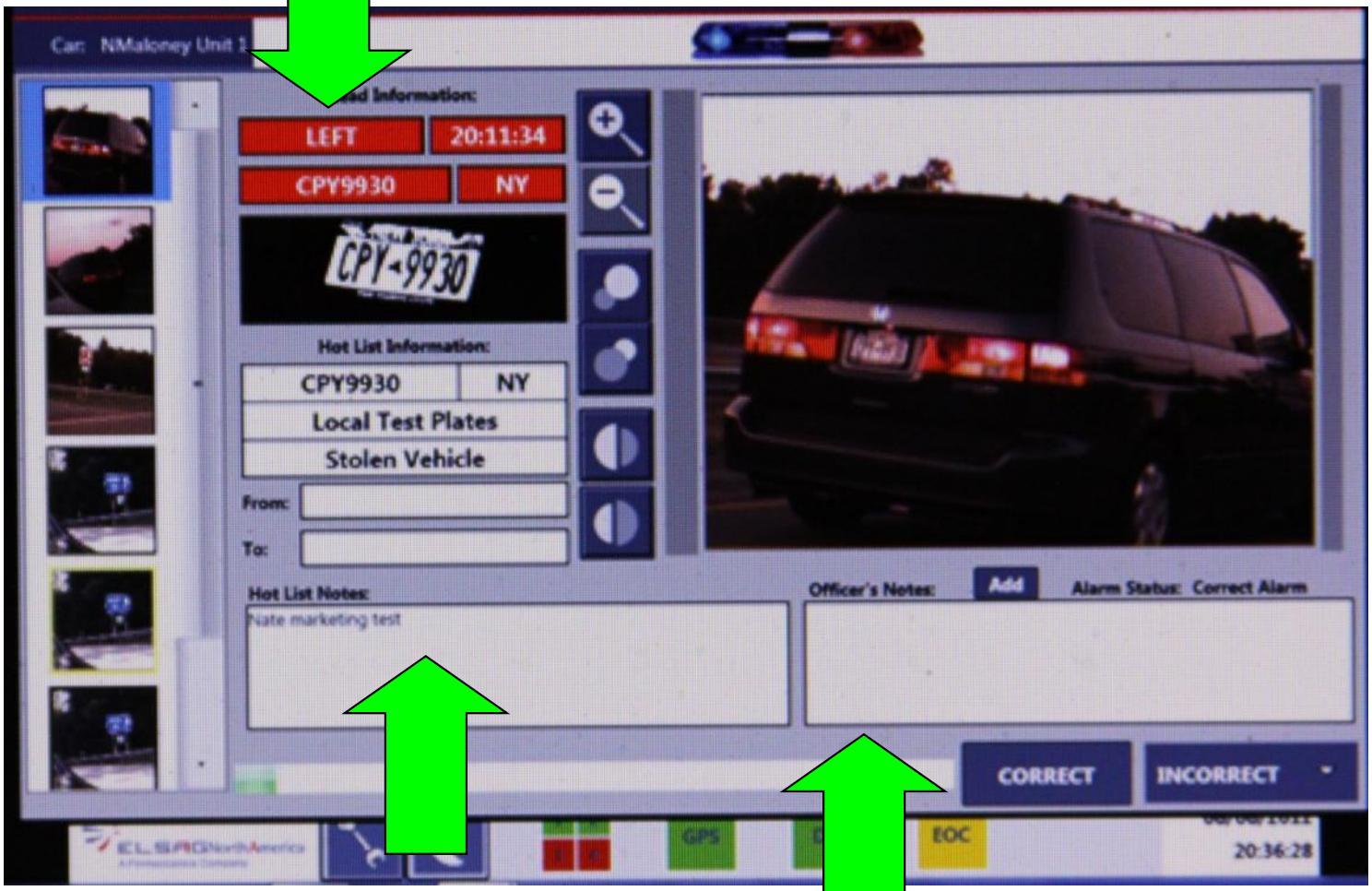
Car System Software Alarm Transaction

Camera side

Real Time Alarms

Audible and Visible

Other pending alarms



Buttons to accept, reject, or correct reads or alarms

Hot List Notes up to 100 characters

Field for officer notes input

© Selex ES Inc., a Leonardo Company

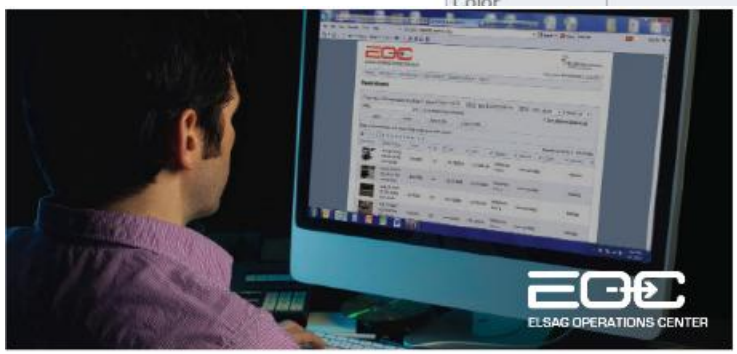
Enterprise Operations Center [EOC] Software for Data Analysis

ENTERPRISE OPERATIONS CENTER

ELSAG

- Collects and Manages ALPR/ANPR data from all cameras together in one integrated system. Real Time uploads to Command Center.
  - Mobile systems
  - Fixed systems
  - Covert systems
- Centralizes and manages your ALPR/ANPR data to support analysis for investigations and intelligence gathering needs.
- Alarms transmitted remotely to users via PC or mobile phones immediately.
- Able to share data with specialized software programs via API.
- Easy Search/Query Functions in Real Time
- Advanced features include data sharing and white list applications.

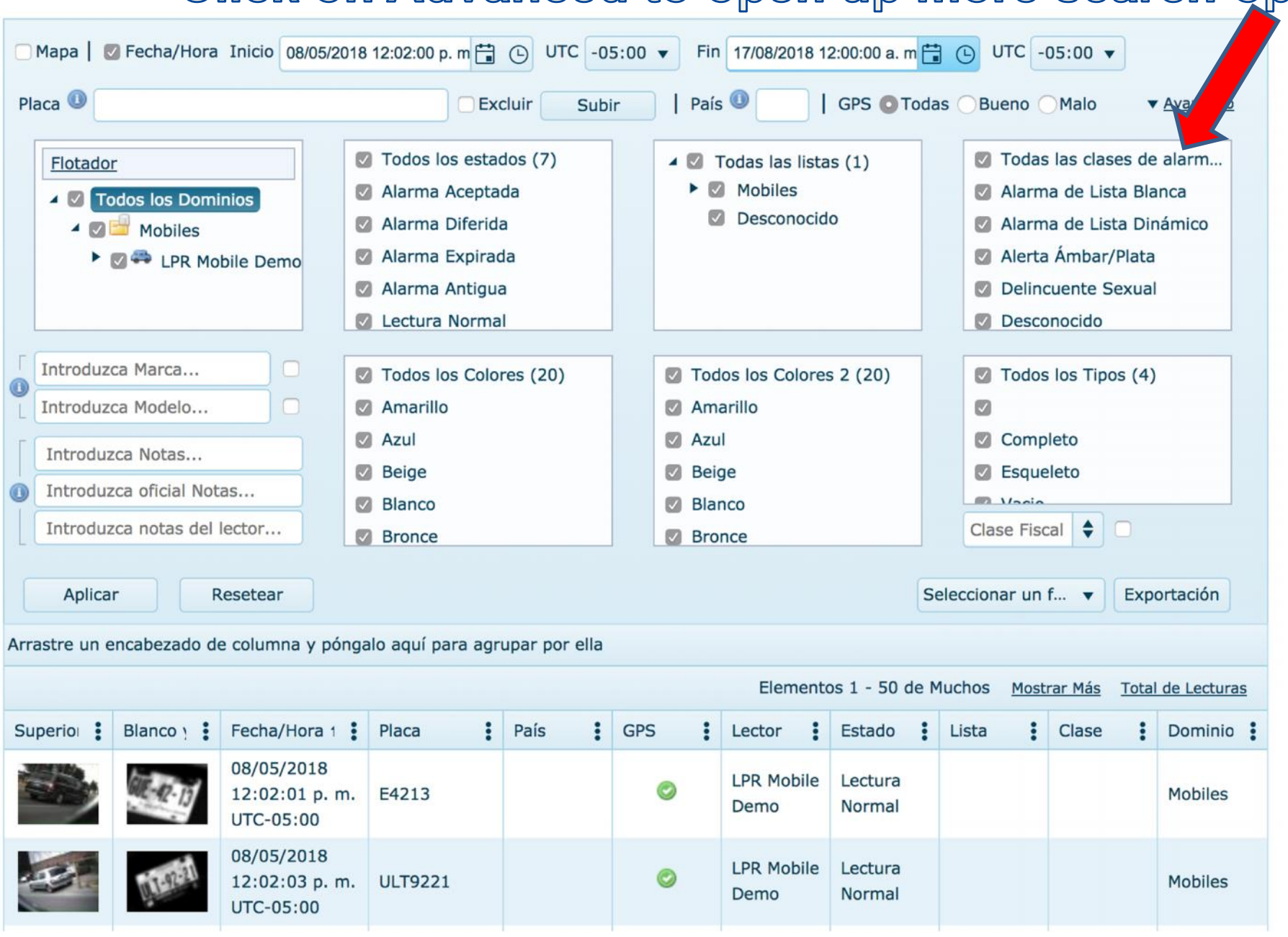




© Selex ES Inc., a Leonardo Company

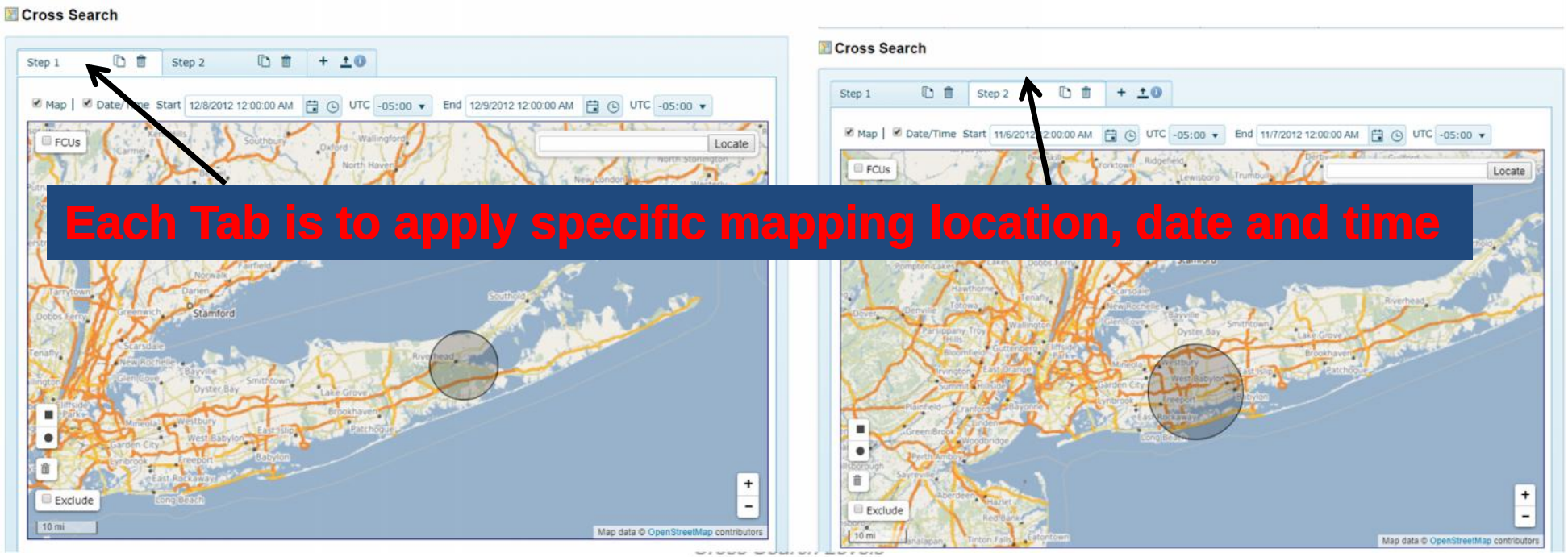
ADVANCED QUERY

Click on Advanced to open up more search options



Cross Search

Burglary suspect seen in multiple locations, matched by date and time of crimes



Each Tab is to apply specific mapping location, date and time

Suspects



Level ×

1 2 3 4 5 6 7 8 9 10 ... 50 1 - 50 of 9299 items

	Overvie	Black &	Date/Time	Plate	Stat	GPS	Reac	Stat	List	Clas	Dom	Leve	Step
Level: 2													
			12/8/2012 1:03:35 PM UTC-05:00	EWX4264	NY		NYSP-Cove...	Normal Read			NYSP	2	1
			11/6/2012 5:47:26 PM UTC-05:00	EWX4264	NY		PoleC...	Normal Read			Nassau PD Surv...	2	2

© Selex ES Inc., a Leonardo Compa

Convoy Analysis

Home | Lists | Data Mining | User Config | System | Monitoring Tools | Help

Reads/Alarms/Convoy Search

Map | Date/Time Start 3/3/2014 12:00 AM End 3/4/2014 12:00 AM UTC -05:00 | Rows 50

Plate

Apply

Clicking on the down arrow runs the convoy search and will display plates that were seen within the time interval selected

Drag a column header and d

1 2 3 4 5 6 7 8 9 10 ...

Displaying items 1 - 50 of 1000 (100000+ Total Reads)

Command	Date/Time	Plate	St	GPS	Reader	Status	List	Class	Domain
	3/3/2014 5:59:44 PM UTC-06:00	757BAD C...			Jcheever Mobile 1	Normal Read			Mid-West
	3/3/2014 5:57:44 PM UTC-06:00								
	3/3/2014 5:57:35 PM UTC-06:00	[D0O]F9M4[... C...			Jcheever Mobile 1	Normal Read			Mid-West Region
	3/3/2014 5:57:26 PM UTC-06:00	158ERE C...			Jcheever Mobile 1	Normal Read			Mid-West Region

Convoy Search

856AVO	8
687HYJ	2
M3294	2

Plate 757BAD has been seen 8 times with plate 856AV0 within 15 seconds of each other

© Selex ES Inc., a Leonardo Company

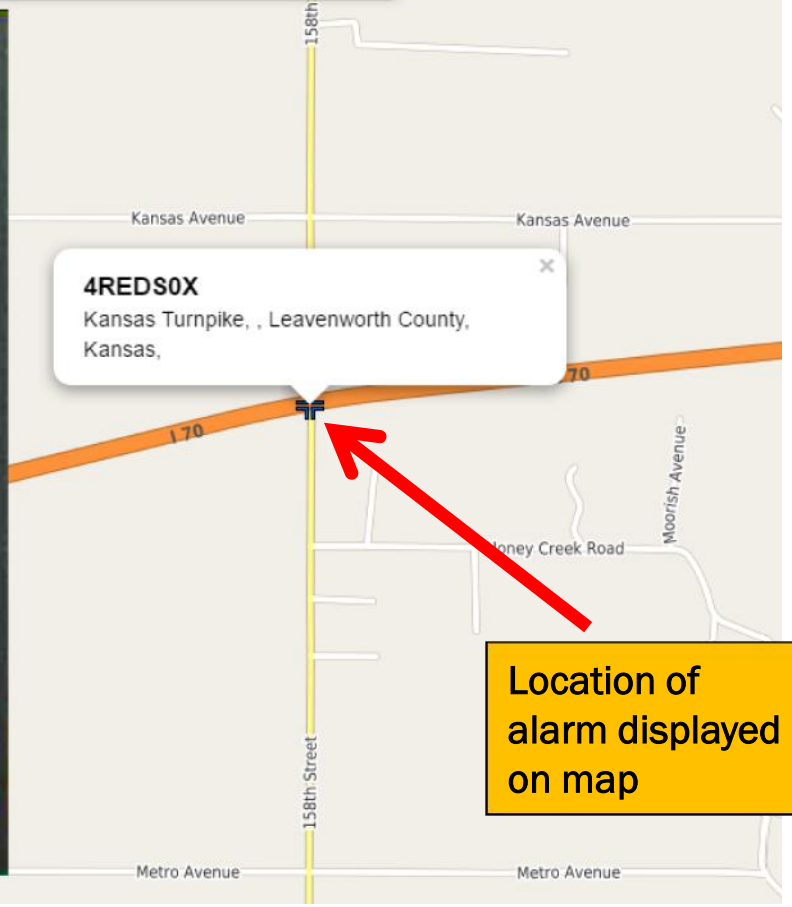
Real Time Updates to Police on Patrol

Alarms | Mute | Center Marker | Compact View | Refresh | Home

Plate	St	Time	Reader	Camera	List	Class	List Notes
4REDS0X	GA	09:59 3/7/2017	I70 Bonner Springs WB	WB Left	Georgia DOR	Other	EXPIRED, FORD , 2007 , FREESTYLE , GRY
DA168B	BC	09:49 3/7/2017	I70 Bonner Springs WB	WB Right	NCIC	Unknown	Unknown Alarm - Canadian Origin - Check NC... akraisi
			I70				



Filters
- Readers
- Classes
- Lists



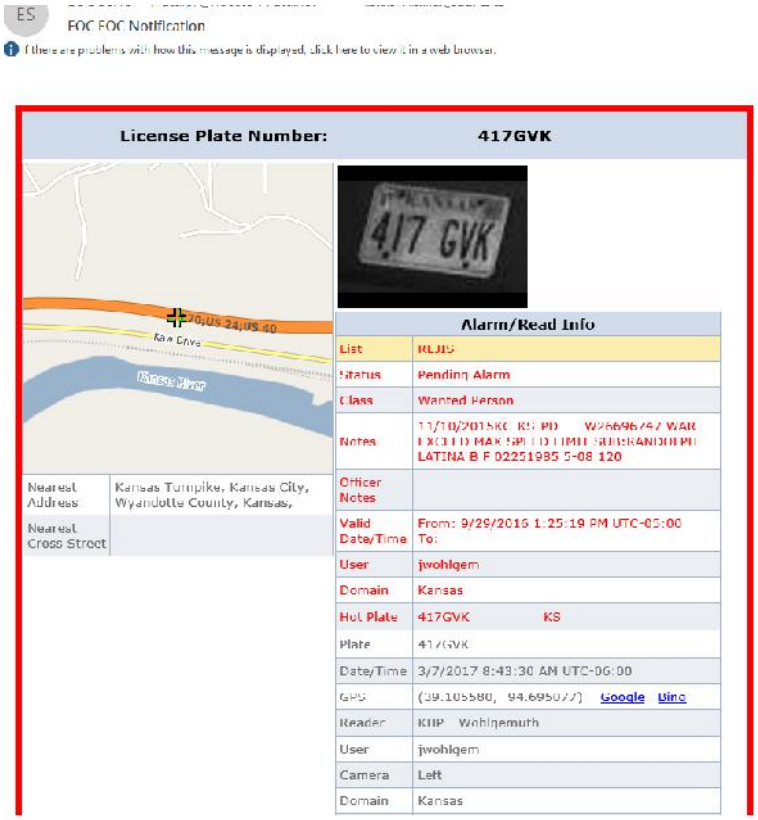
Click plate or color image to enlarge

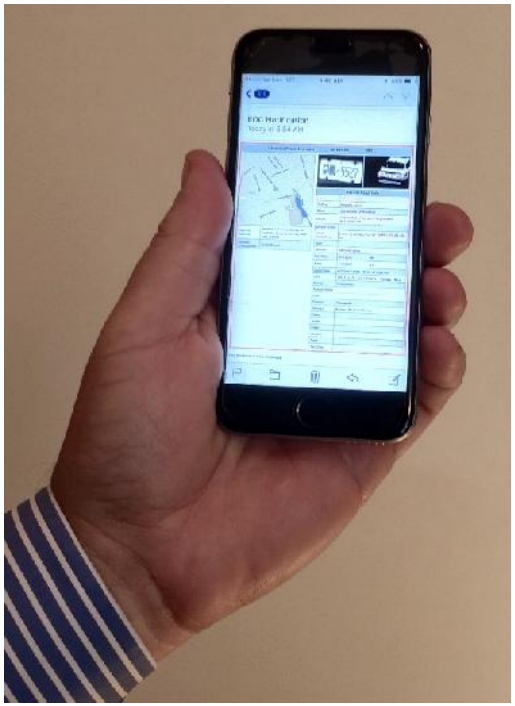
Location of alarm displayed on map

© ELSAG 2018

EOC

ENTERPRISE OPERATIONS CENTER





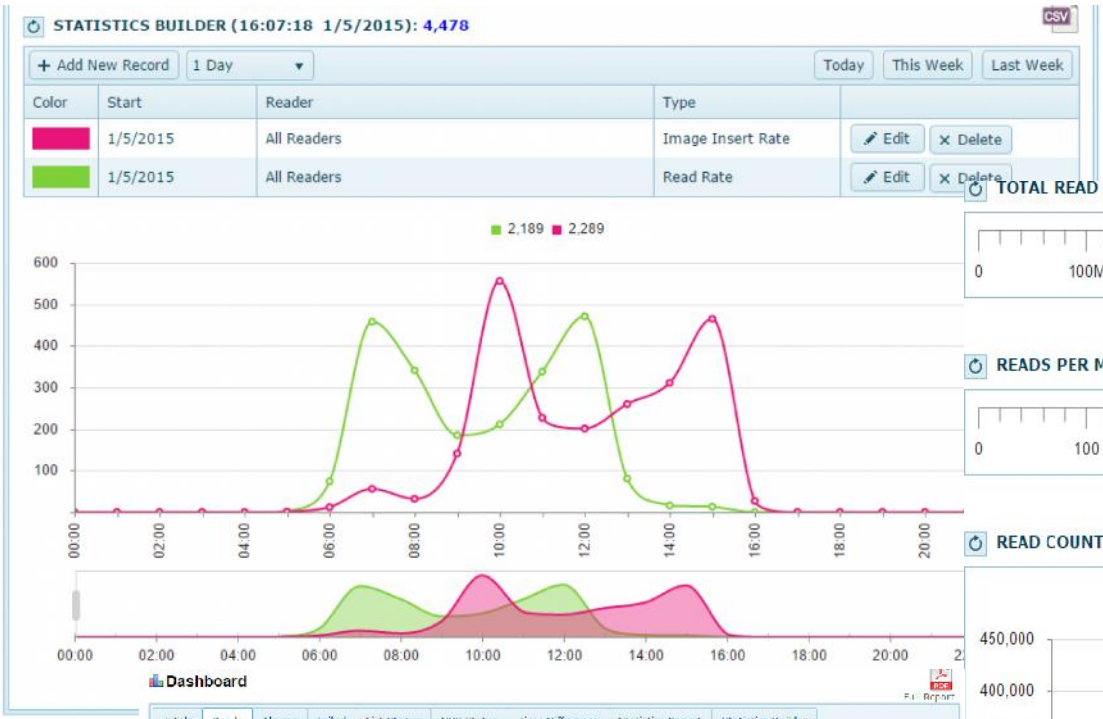
Receive email critical notifications of important alarms directly to your smartphone.

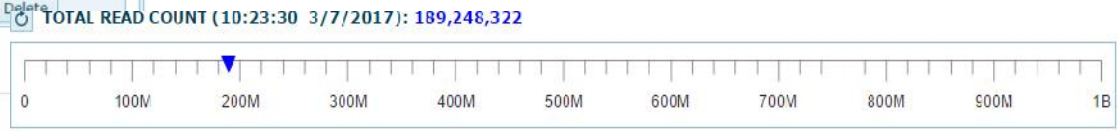
Includes a link to go directly to the server.

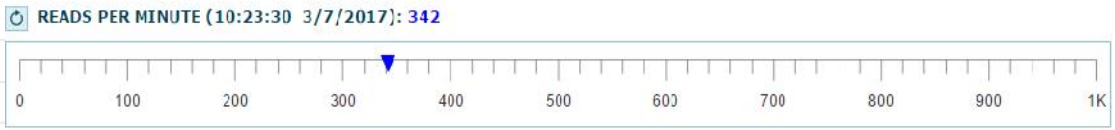
- **Missing Children & Seniors**
- **Kidnapping victims**
- **Terrorist incidents**
- **Real Time Alerts in your Pocket**

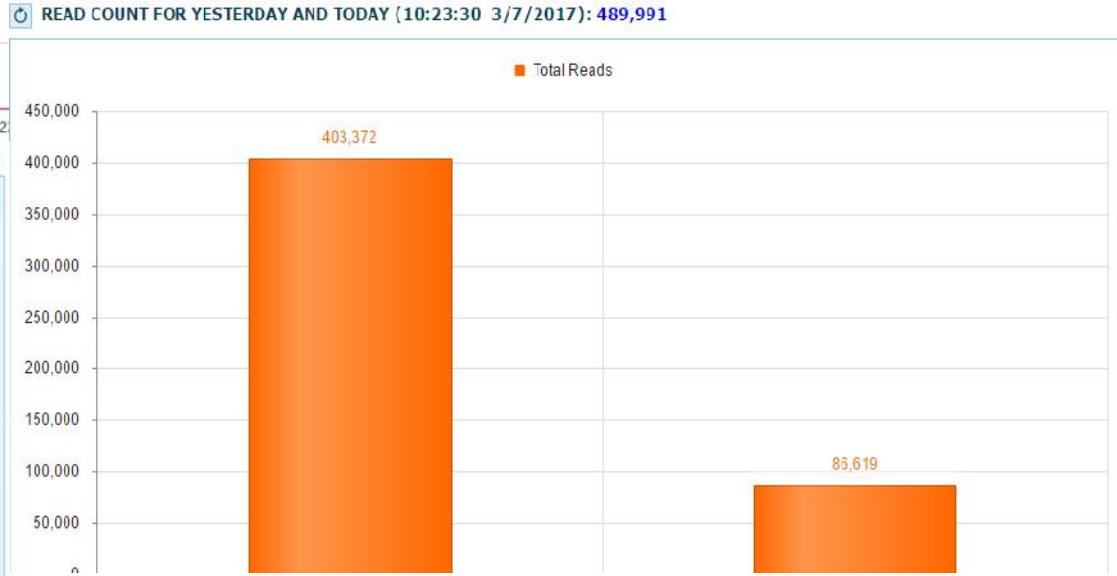
© Selex ES Inc., a Leonardo Company

Analytics











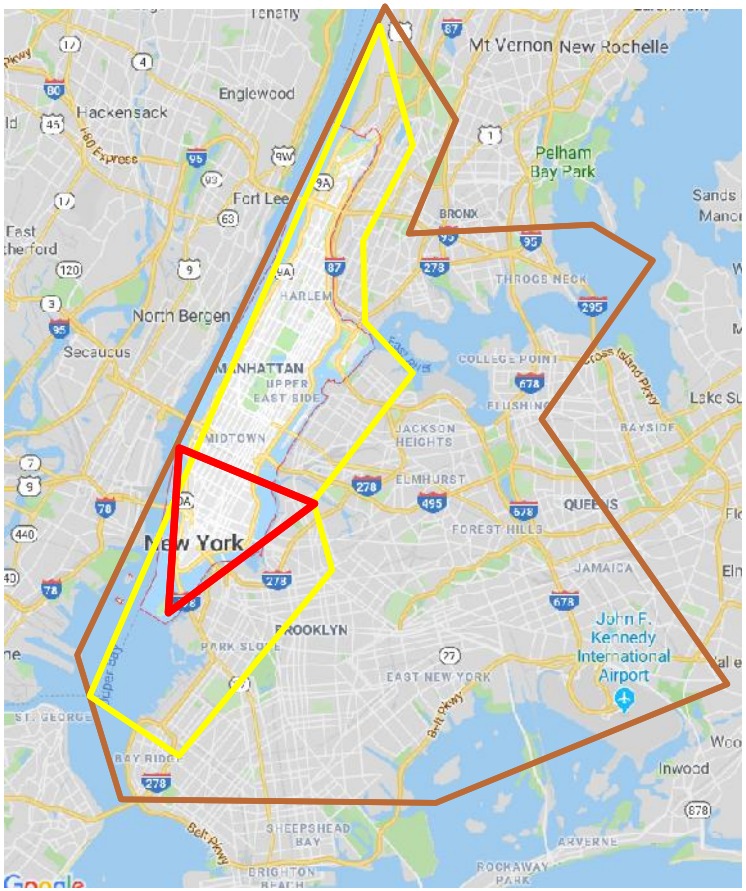
© Selex ES

Key Deployments 4500+ law enforcement customers

- NYPD (New York City Police Department)
- DEA (Drug Enforcement Agency) & HIDTA
- US President & Congress Secret Service
- Washington DC Capitol Protection Mission
- Italian Carabinieri
- Policia Metropolitana Buenos Aires Argentina
- FBI
- CISEN Mexico (Mexico equiv. of FBI)
- United Kingdom Home Office
- Royal Malaysia Police
- Queensland Police Australia
- US Army, US Navy NCIS, US Marines

70% of U.S. market :
50 states and all Federal Agencies
30+ Countries throughout world

ALPR Protection of New York City



NYPD New York City Police Department

> 600 fixed and mobile ALPR cameras

All bridges and tunnels ; 100% entry / exit into City

3.2 Million/day reads to NYPD Real Time Crime Center

3 ‘Rings of Steel’ to contain threats to :

- Wall Street Financial Center
- World Trade Center
- Times Square
- 12 Million residents and tourists

Predictive Intelligence-led Policing for Public Safety

Port Authority, Metropolitan Transportation Authority

Premium 24/7/365 Support; updates & tech refresh

Weekly Police user input and enhancements

© Selex ES Inc., a Leonardo Company

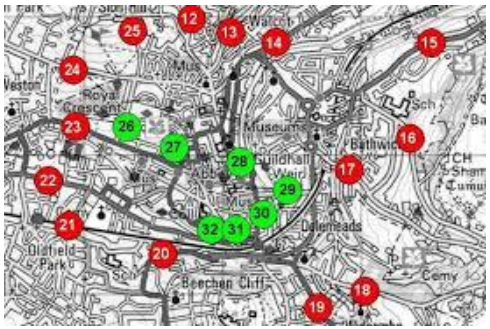
United Kingdom - EOC

Home Office



- National ANPR Service (NAS)

- 120 Million Plates/Day (>40B/Year)
- Cities, Counter Terror, MI5, MI6
- 40,000+ users nation-wide
- Integration of different LPR camera makes
- One Centralized EOC server; largest in World



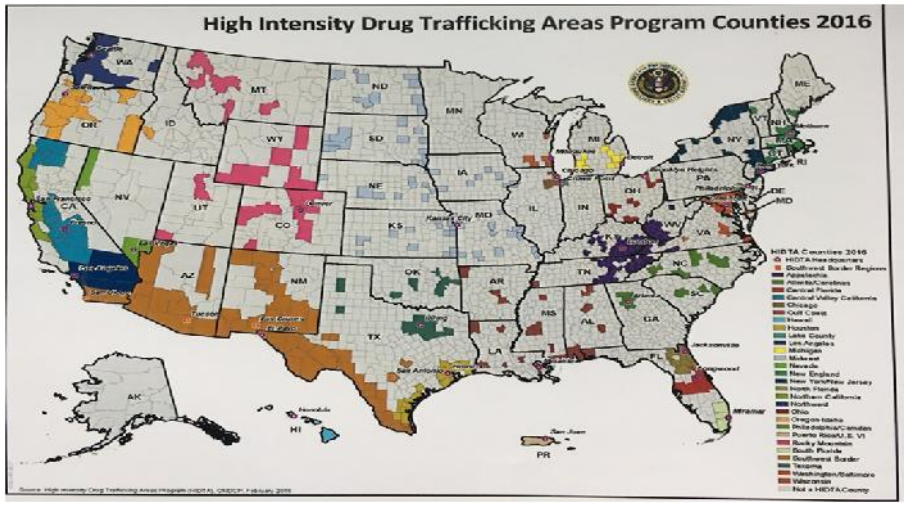


© Selex ES Inc., a Leonardo Company

High Intensity Drug Trafficking Area

The HIDTA program, in conjunction with the DEA, provides assistance to Federal, State, Local, and tribal law enforcement agencies operating in areas determined to be critical drug trafficking regions of the Nation.

- Currently 28 regional HIDTA agencies which include approximately 16 percent of all counties in United States and 60 percent of the population.
- Representatives of Federal, State, Local, and Tribal agencies in each HIDTA region coordinate and collaborate to address the specific drug and human trafficking threats of that region.



© Selex ES Inc., a Leonardo Company

Benefits of Tracking Vehicles



Welding Truck smuggling 2.5 Million Cash captured by using HIDTA EOC March 2017



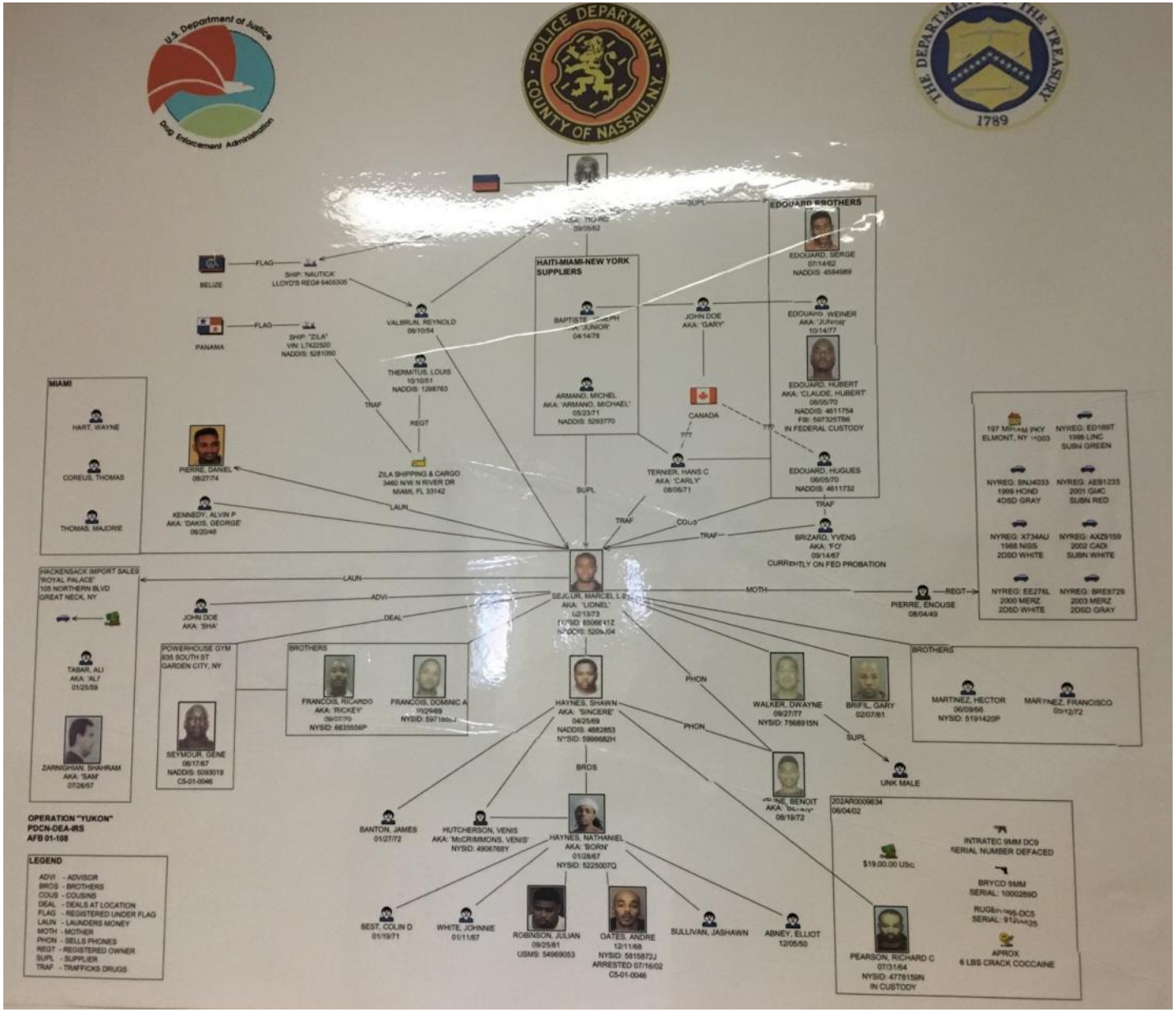
Interstate 10 Texas 2.0 Million Cash captured by using HIDTA EOC June 2017

HIDTA/DEA is an Asset and Forfeiture organization which means that they can retain and re-invest portions of cash which they capture from criminals to re-invest in technology

© Se

New York Drug and Gang Task Force

Using Elsag EOC software for analysis in order to create movement and relationship based intelligence on Drug Cartels and other Organized Crime Gangs



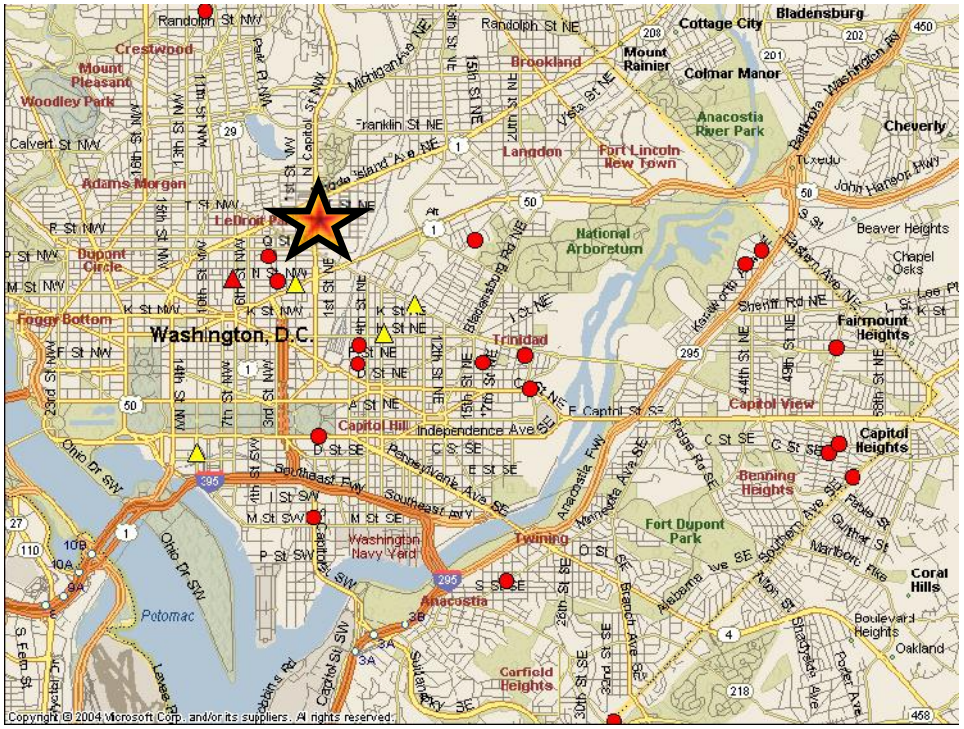
© Selex ES Inc., a Leonardo Company

Elsag protects Washington DC

Sole ALPR provider for National Capitol Protection Program with over 1000 cameras deployed in Capitol Region feeding to Dept. Homeland Security.

example of results from one shift

Total Reads	59,650
Average total Patrol Time for 5 vehicles	21 Hours
Stolen Vehicles Recovered	**38**
Carjacking Vehicles Identified	5
Tractor Trailers	1
Stolen Plates Recovered	**14**
# of Bench Warrant Alarms	**2**
Total Alarms with Interdiction	**54**
Average Time between alarms	23m:20s
# of Guns Recovered	3
# of current arrests	**18**



2 Drug Seizures

Seizure #1 - 62grams of Crack Cocaine

Seizure #2 - 30 Separate Rocks of Crack Cocaine + 2 Zips of Crack Measuring and Packaging Devices

Stolens of Note

Stolen Tractor Trailer reported stolen in Massachusetts found in Capitol Mall, DC.

Seized on U.S. Capital Building Grounds (National Security)–

#1 Stolen Late Model Truck 8:34 AM 101 Constitution

#2 Stolen Taxi Cab 6:15 PM Rayburn Office Building

© Selex ES Inc., a Leonardo Company

Summary of Uses : MPH FPH & EOC



INTERDICTION

- Stolen Vehicles
- Wanted Persons
- Suspended/Revoked Drivers
- Drug/Guns/Money Seizures
- Missing Persons / Kidnap

INTELLIGENCE

- Tracking Organized Crime Gangs /Racketeering
- Persons of Interest
- Crime Scene Investigation Tool
- Terrorist Watch/Homeland Security Investigations

INCOME

- Asset Forfeitures & Fines
- Traffic Fines Due
- Tax Collection

© Selex ES Inc., a Leonardo Company

PSE01: Public Safety Equipment and Two-Way Radio

UPDATED: 02/17/2023

Contract #:	PSE01
MMARS MA #:	PSE01*
Initial Contract Term:	January 1, 2022, to December 31, 2026
Maximum End Date:	One (1) option for two (2) year extension through December 31, 2028
Current Contract Term:	January 1, 2022, to December 31, 2026
Contract Manager:	Kelly Thompson Clark, 617-720-3184, kelly.thompsonclark@mass.gov
This Contract Contains:	Environmentally Preferable Products, Small Business Purchasing Program, MBE/MWBE/WBE, Service-Disabled Veteran-Owned Business
UNSPSC Codes:	**Fire:** 46-16-00, 46-19-00 **EMS:** 42-17-00, 42-17-22 **Police:** 46-20-00, 92-10-15 **Marine:** 25-11-00, 92-12-19 **Two-Way Radio's:** 43-19-15, 43-19-16, 43-22-17, 81-11-18

Table of Contents:

(NOTE: To access hyperlinks below, scroll over desired section and CTL + Click)

- Contract Summary
- Contract Categories
- Benefits and Cost Savings
- Find Bid/Contract Documents
- Who Can Use This Contract
- Subcontractors
- Construction Requirements
- Supplier Diversity Requirements
- Pricing, Quotes and Purchase Options
- Instructions for MMARS Users
- Performance and Payment Time Frames Which Exceed Contract Duration
- Environmentally Preferable Products
- Contract Exclusions and Related Statewide Contracts
- Emergency Services
- Shipping/Delivery/Returns
- Additional Information/FAQ's
- Strategic Sourcing Team Members
- VENDOR LIST AND INFORMATION
- Appendix A: UNSPSC Codes for PSE01

TIP: To return to the first page throughout this document, use the CTL + Home command.

Contract Summary

This is the Statewide Contract for Public Safety Equipment and Two-Way Radio supplies and services. This new Statewide Contract replaces and combines the public safety and two-way radio categories from statewide contract numbers FIR04/FIR04A and ITT57. OSD has rebranded the "FIR" and two-way radio statewide contracts to create a brand-new contract category entitled "PSE" to offer a single and cohesive contract for all public safety equipment, supplies and applicable services. The contract category "FIR" will no longer be used as a category of services.

COVID-19 Updates

As the CDC has found that COVID-19 is contracted primarily through airborne transmission, organizations may wish to reevaluate cleaning protocols and apply disinfectants to surface areas only as needed. Disinfectants used for this purpose should be listed on EPA's List N: Disinfectants for Use Against SARS-CoV-2, and it is recommended to choose safer disinfectants (find more information about safer disinfectants on the Toxics Use Reduction Institute's COVID-19: Safely Clean & Disinfect webpage) which may be found on the FAC118: Environmentally Preferable Cleaning Products, Programs, Equipment and Supplies contract. In addition, hand sanitizers must contain at least 60% ethanol per the Centers for Disease Control (CDC) guidance.

Contract Categories

This contract includes 5 categories of Public Safety Equipment and Two-Way Radio products/service as listed below:

- Category 1: Fire Equipment, Supplies, and Services
- Category 2: Emergency Medical Services (EMS) Equipment, Supplies, and Services
- Category 3: Police Equipment, Supplies, and Services
- Category 4: Marine Equipment, Supplies and Services
- Category 5: Two-way Radio Equipment, Supplies and Services

PLEASE NOTE: The items identified below **cannot** be purchased under the PSE01 Public Safety Equipment and Two-Way Radio, Supplies, Services and Repairs statewide contract:

- Firearms, Ammunitions, Related Training Products, Services Accessories and Less than Lethal Munitions, Tasers, etc.
- All vehicles including fire trucks and boats.
- Public Safety Broadband and LTE only communications equipment and services (the home Statewide Contract for this is ITT72).

Benefits and Cost Savings

Statewide contracts are an easy way to obtain benefits for your organization by leveraging the Commonwealth's buying power, solicitation process, contracting expertise, vendor management and oversight, and the availability of environmentally preferable products.

The statewide contract covers a broad array of public safety equipment, parts & services available through various authorized dealers of listed manufacturers. Competitive Pricing – The Strategic Sourcing Services Team (SST) has awarded the contract to those Contractors who provided the most competitive discounts for the manufacturers being offered. Complete award information for awarded Contractors is located in COMMBUYS https://www.commbuys.com/bso/advsearch/buyerAdvancedSearch.sdo. Please see instructions below for how to obtain the contract information in COMMBUYS.

Vendors on the PSE01 statewide contract also offer the following discounts which can vary for each Vendor: Prompt Pay Discounts, Dock Delivery Discounts, Volume Discounts, Trade-In's.

Find Bid/Contract Documents

- To find all contract-specific documents, including the Contract User Guide, RFR, specifications, and other attachments, visit COMMBUYS.com and search for PSE01 to find related Master Blanket Purchase Order (MBPOs) information. All common contract documents are located in the "Master Contract Record" Master Blanket Purchase Order (MBPO) for PSE01 and can be accessed directly by visiting [list the Master MBPO hyperlink here, for example, Master Blanket Purchase Order PO-15-1080-OSD01-OSD10-00000003619].
- To find vendor-specific documents, including price sheets, see links to individual vendor MBPOs on the Vendor Information page.

Who Can Use This Contract

Applicable Procurement Law

Executive Branch Goods and Services: MGL c. 7, § 22; c. 30, § 51, § 52; 801 CMR 21.00
Construction Materials and Services: G.L. c. 149, s. 44A; G.L. c. 30, § 39M

Eligible Entities

Please see the standard list of Eligible Entities on our Eligible Entities Which May Use Statewide Contracts webpage.

Subcontractors

The awarded vendor's use of subcontractors is subject to the provisions of the Commonwealth's Terms and

Conditions and Standard Contract Form, as well as other applicable terms of this Statewide Contract.

Construction Requirements

Purchasers must ensure that **any** services involving construction are limited to $50,000 or less.

Purchasing entities are responsible for compliance with applicable construction law requirements. Information concerning specific , M.G.L. c. 149 and c. 30 construction requirements may be found in the Office of the Inspector General's Public Procurement Charts at: https://www.mass.gov/download-oig-public-purchasing-and-public-construction-manuals. It is the responsibility of the Eligible Entity to determine whether installation work includes construction as defined by M.G.L. c.149 or M.G.L. c.30, §39M. Chapter 30B Procurement Assistance from the Office of the Inspector General is available at https://www.mass.gov/how-to/get-public-procurement-assistance-from-our-chapter-30b-team. Access the 30B Hotline at 617-722-8838 or by email at: 30BHotline@mass.gov.

Questions about public construction bidding should be directed to Deborah Anderson, Counsel II for the Attorney General's Office, at 617-963-2371. Visit the Attorney General's Public Construction web page to learn more about Public Bidding Laws.

See Quotes Including Construction Services Requirements below for information on quoting these types of projects.

Supplier Diversity Requirements

When selecting contractors and placing orders, Executive departments shall utilize diverse and small businesses to the extent possible based on contract terms, SDO and departmental policies, laws, and regulations. Additionally, departments shall make a preference for contractors with higher SDP commitments and/or performance whenever such information is available (or is requested from contractors by the department) and the preference is feasible.

OSD provides up-to-date information on the availability of diverse and small businesses on statewide contracts through the Statewide Contract Index available on the COMMBUYS home page. See the "Programs (SDO and SBPP)" tab for current certification and small business status of contractors on this contract.

Pricing, Quote and Purchase Options

Purchase Options

The purchase options identified below are the only acceptable options that may be used on this contract:

- Purchases made through this contract will be direct, outright purchases

- This is a fee for service contract
- Product pricing may be found on the vendor information page, where links to all the vendors MBPOs are provided.

Pricing Options

- **Discount off Manufacturers Suggested Retail Price (MSRP):** Contract pricing is a specified discount off the MSRP* catalog price. Further negotiations can be made based on volume as PSE01 offer volume-based discounts.

**Please note not all items have a static MSRP price list. Due to varying brands and base models an exhaustive list of MSRPs is not always possible however, a vendor should always provide a quote showing a base price, your contracted discount and final contracted pricing.*

Product/Service Pricing and Finding Vendor Price Files

Manufacturer's Suggested Retail Price (MSRP) Files on COMMBUYS

At times during the duration of this contract, some PSE01 Vendors may have outdated MSRP* reference files on COMMBUYS. Because of this, Buyers should always request that a vendor provide them the most current MSRP at the time of quote. Buyers may then refer to the awarded vendor's PSE01 price file from COMMBUYS to check pricing. All Vendors have an awarded price file in Microsoft Excel format that indicates their approved manufacturers and their awarded discount off of MSRP for their starting price. If a vendor does not have a manufacturer listed in their awarded PSE01 price file, the vendor must work with OSD to get that manufacturer added before they can sell their products on PSE01. If a vendor is not honoring their discount pricing from the PSE01 price file, then the customer should contact the OSD Contract Manager.

**Please note not all items have a static MSRP price list. Due to varying brands and base models an exhaustive list of MSRPs is not always possible however, a vendor should always provide a quote showing a base price, your contracted discount and final contracted pricing.*

Setting Up a COMMBUYS Account

COMMBUYS is the Commonwealth's electronic Market Center supporting online commerce between government purchasers and businesses. If you do not have one already, contact the COMMBUYS Help Desk to set up a COMMBUYS buyer account for your organization: (888)-627-8283 or OSDhelpdesk@mass.gov.

When contacting a vendor on statewide contract, always reference PSE01 to receive contract pricing.

Quick Search in COMMBUYS

Log into COMMBUYS and use the Search box on the COMMBUYS header bar to locate items described on the MBPO or within the vendor catalog line items. Select Contract/Blanket or Catalog from the drop-down menu.

How to Purchase from the Contract

- This contract has been set up as a distributor model (solicitation enabled) Master Blanket Purchase Order (MBPO) in COMMBUYS. A Solicitation Enabled Distributor Model MBPO is a single MBPO that has multiple Vendors listed as distributors. This allows you to solicit quotes within COMMBUYS, award and place the order through COMMBUYS.

  There are fifty - five (55) total Vendors on this contract and five (5) different distributor model Master Blanket Purchase Orders (MBPO). Each Vendor MBPO contains a list of Vendor specific files. The Master Contract Record MBPO is a non-purchasing MBPO housing all pertinent SWC records including the Contract User Guide and the Statement of Work Template.

  The five (5) different distributor model Master Blanket Purchase Orders (MBPO) numbers are below, it allows buyers to solicit quotes from multiple vendors on PSE01:

  - **Category 1:** Fire Public Safety Equipment = **PO-22-1080-OSD03-SRC3-24071**
  - **Category 2:** EMS Public Safety Equipment = **PO-22-1080-OSD03-SRC3-24070**
  - **Category 3:** Police Public Safety Equipment = Solicitation Enabled MBPO = **PO-22-1080-OSD03-SRC3-24061**
  - **Category 4:** Marine Public Safety Equipment = Solicitation Enabled MBPO = **PO-22-1080-OSD03-SRC3-24067**
  - **Category 5:** Two Way Radio Public Safety Equipment = Solicitation Enabled MBPO = **PO-22-1080-OSD03-SRC3-24068**

  This COMMBUYS functionality provides a mechanism to easily obtain quotes, as specified by the Contract. The buyer would create a Release Requisition, and then convert it to a Bid. After approval by the buyer approving officer, the bid is then sent to selected vendors to request quotes. Buyers must include “PSE01 RFQ” when entering information in the Description field.

- **Select items from a PunchOut catalog and purchase through COMMBUYS**

  PunchOut catalogs offer the convenience of selecting Statewide Contract products from a vendor’s e-commerce website. The PunchOut or Government to Business (G2B) catalogs are available via COMMBUYS

only (login to COMMBUYS and select the settings option in the upper right-hand corner [] and choose the G2B PunchOut option). Once a vendor is selected in COMMBUYS, you are taken to the vendor's e-commerce site. After shopping is complete on the vendor's e-commerce site, selected items are pulled back into COMMBUYS, summarized on a COMMBUYS release Requisition, and are ready to submit for approval. Once approved, it is released to the vendor for processing and fulfillment.

For a description of how to complete this purchase in COMMBUYS, visit the Job Aids for Buyers webpage and select either:

- The Quick Reference Guide (QRG) section and choose the QRG – Creating a Punch Out Order job aid
- The COMMBUYS Purchase Orders section and choose the How to Purchase from a COMMBUYS PunchOut job aid.

- **Directly purchase a non-fixed price item ($0 line item) through COMMBUYS**
  All vendor MBPO pages have a $0.00 line item for placing orders. When placing an order in COMMBUYS a contract user needs to type in the total cost of the order and may add invoice/quote information as reference either by typing in the information or attaching as a PDF file.

  For a description of how to complete this purchase in COMMBUYS, visit the *Job Aids for Buyers* webpage and select:
  - The *COMMBUYS Requisitions* section, then choose the *Make a Statewide Contract Purchase in COMMBUYS* job aid.

Obtaining Quotes

Contract users should always reference PSE01 when contacting vendors to ensure they are receiving contract pricing. Quotes, not including construction services, should be awarded based on best value.

For a full description of how to complete a quote in COMMBUYS visit the Job Aids for Buyers webpage, and select:

- The COMMBUYS Purchase Orders section, then choose Request Quotes from Vendors on Statewide Contracts job aid.

Quotes Including Construction Services

Please note specific requirements that apply for quoting construction services, depending upon the scope of your bid:

- Where the construction services are less than $10,000: Select a vendor based on sound business practices, consistent with your entity's procurement policies and procedures.

- For construction services valued from $10,000-$50,000: Must solicit a minimum of three quotes and receive two written responses; award to lowest responsible bidder.

Quotes Not Including Construction Services:

Award based on best value, but it's strongly encouraged that Entities solicit at least three quotes from Vendors to be evaluated with best value criteria applied.

Prevailing Wage Requirements

The Massachusetts prevailing wage laws require that covered employees on public works projects be paid a minimum hourly rate set by the Department of Labor Standards (DLS). The prevailing wage laws apply to both union and non-union employers and employees. The buyer has a legal obligation to request a prevailing wage schedule from the Department of Labor Standards (DLS) at www.mass.gov/dols. To get the proper rates for your region/job, you must request a determination. Questions regarding the Prevailing Wage Law may be answered by accessing the DLS website or by calling the DLS Prevailing Wage Program at (617) 626-6953.

If prevailing wage is required, make sure to include this information in your quotes or bids so vendors know to include prevailing wage.

In addition, all contracts by a state agency or state-assisted contracts for design, construction, reconstruction, installation, demolition, maintenance, or repair must contain Workforce Participation Goals for minorities and women. This is required by M.G.L. c. 149, § 44A(2)(G). A "state-assisted contract" is a construction project undertaken by a political subdivision of the Commonwealth or two or more subdivisions thereof for planning, acquisition, design, construction, demolition, installation, repair, or maintenance whose costs are paid for, reimbursed, grant funded, or otherwise supported, in whole or in part, by the Commonwealth. An affected awarding authority's bid documents must include a reference to the specific goals that will be contained in the contract. The contract must also include the processes and procedures to ensure compliance with the Workforce Participation Goals, including reporting and enforcement provisions. For questions about the Workforce Participation Goals law, please contact Deborah Anderson at the Attorney General's Office at 617-963-2371 or visit the Attorney General's Public Construction Bidding in Massachusetts FAQ.

The Office of the Attorney General's Fair Labor Division is responsible for enforcing the prevailing wage laws. Visit www.mass.gov/prevailing-wage-enforcement for more information.

Instructions for MMARS Users

MMARS users must reference the MA number in the proper field in MMARS when placing orders with any contractor. Contact the Comptroller Help and Support Desk at 617-973-2468 or via email at Comptroller.Info@mass.gov for additional support.

Environmentally Preferable Products (EPP)

GreenScreen certified firefighting foams, which have been tested to be both free of Per- and polyfluoroalkyl substances (PFAS) and free of the chemicals of highest health and environmental concerns, are now available through this contract.

EPP Requirements:

State buyers are reminded that Environmentally Preferable Products (EPP) Procurement Program requirements for the use of environmentally preferable disinfectants, and some cleaning supplies, has been waived due to the availability of the products impacted by the demand caused by COVID-19. As the EPP supply replenishes, buyers are reminded that these disinfectants and other third-party certified products remain recommended for use and are selected for public health and environmental standards. For additional guidance, visit the Toxics Use Reduction Institute's COVID-19: Safely Clean & Disinfect webpage.

Contract Exclusions and Related Statewide Contracts

The items identified below **cannot** be purchased under the PSE01 Public Safety Equipment, Supplies, Services and Repairs statewide contract:

- Firearms, Ammunitions, Related Training Products, Services Accessories and Less than Lethal Munitions, Tasers, etc.
- All vehicles including fire trucks and boats.
- Public Safety Broadband and LTE only communications equipment and services (the home Statewide Contract for this is ITT72).

Emergency Services

Many statewide contracts are required to provide products or services in cases of statewide emergencies. ML - 801 CMR 21 defines emergency for procurement purposes. Visit the Emergency Response Supplies, Services and Equipment Contact Information for Statewide Contracts list for emergency services related to this contract.

Shipping/Delivery/Returns

All quotations shall be FOB destination. The term FOB destination shall mean delivered and unloaded to all the Commonwealth Departments, cities, towns and/or Political Subdivisions within the Commonwealth of Massachusetts, with all charges for transportation and unloading prepaid by the Contractor(s).

The Contractor(s) must deliver goods to the Department requesting the goods within 30 days after receipt of order (A.R.O.). Items delivered after 30 business days may be deemed unacceptable and returned to the Contractor at no cost to the Commonwealth. Delivery arrangements for custom-made items may be made by mutual agreement between purchasing Department and Contractor(s).

Surcharges: Vendors will not charge any additional fuel, shipping, transportation, energy*, insurance or any other type of surcharge or fee on any order received from departments. Departments will NOT be required to pay any additional surcharges upon receipt of contractor invoicing. **Cylinder Fees are allowed under this contract.*

At the discretion of the Commonwealth, shipping charges may be negotiated and allowed under extenuating circumstances including, but not limited to: rush shipping requests by the Commonwealth Agency, oversized or heavy items being repaired, etc. This exception will only be allowed with an Agency request. Vendors are not allowed to request an exception for shipping charges.

Additional Information/FAQs

Performance Bond

User Departments may request and require Contractors to furnish a performance and/or labor and materials bond, in a form and with surety satisfactory to the end user for those orders in the amount of $100,000 or more. The Contractor(s) shall be responsible for the cost of the bond(s).

Adding/Removing Products

The SST reserves the right to add products on an as needed basis despite their initial exclusion. Contractors must obtain authorization from OSD in order to add a product to the contract award. The products should comply with the specifications and scope/description established in the original Request for Response (RFR) and the Contractor must supply all supporting information and research available to the SST for consideration. A written recommendation may also be submitted to the SST from an eligible contract user requesting that specific brands and/or manufacturers' products be added to the contract. NO PRODUCTS MAY BE ADDED WITHOUT APPROVAL OF THE SST AND SSM.

Frequently Purchased Items on the Contract:

Fire Equipment & Supplies

Turnout gear, Urban Search and Rescue (USAR) gear, station work uniforms, dress uniforms, specialized outerwear, forestry clothing, any other firefighter personal protective equipment (PPE), self-contained breathing apparatus (SCBA) and SCBA cylinders, breathing air compressors, SCBA test benches, SCBA fit testers, self-contained smoke/fire hoods, firefighting foam, water applications (hoses, nozzles, gates), ladders, power tools, hand tools, emergency vehicle lighting, specialty equipment (meters, including air monitoring, radiological, etc., meter calibration equipment, meter calibration gases and meter parts; other types of specialty gas, bottled or otherwise, not currently covered under ENE46, HSP41 or their successor contracts), fire alarm equipment (control panels, smoke/heat devices, water flow devices, signaling, receiving and cabling items), associated software updates, training aids and not limited to the items identified. Services and/or repairs of any or all of the above listed items. (All vehicles excluded).

EMS Equipment & Supplies

Emergency and field EMS products, plus medical equipment and supplies used by first responders and all levels of EMT certification. Includes disaster management products, extrication, immobilization and transportation products, airway management equipment, resuscitation products, emergency and field medical services kits, EMS supplies, cardiac monitors, IV pumps, transport ventilators, assessment equipment (blood pressure units, pulse oximeters, thermometers, exam lights), associated software updates, training aids and not limited to the items identified. Services and/or repairs of any or all of the above listed items. (Excludes vehicles, medications, and drugs).

Police Equipment & Supplies

Night vision binoculars, breathalyzers, visibility clothing, firearms lockers, patrol car recording devices, GPS tracking devices, license plate recognition equipment, gloves, knee pads, helmets, handcuffs, tactical mirrors, vehicle emergency lights, sirens, body cameras, traffic and crowd control equipment, forensic equipment, helium, and acetylene gases, associated software updates, training aids, and not limited to the items identified. Services and/or repairs of any or all of the above listed items. (Excluded from this contract are the following: weapons, ammunition, lethal and less than lethal munitions, tasers and all vehicles).

Marine Equipment & Supplies

Equipment and supplies for the Maritime Incident Response Teams for port security, incident response, water training events, etc. including dry suits, multi-threat suits, personal floatation devices (PFDs), emergency position indicator radio beacons (EPIRBs), dry bags, marine ropes, re-breather apparatus, marine communication equipment, waterproof night vision cameras, marine locator equipment, craft systems and repair equipment,

scuba and snorkeling gear, swim equipment and not limited to the items identified. Services and/or repairs of any or all of the above listed items. (Excludes all boats and vehicles).

Two Way Radio Repairs and Services

Purchase, rental, installation, maintenance and service of Two-Way Radio and associated microwave radio systems, equipment, connected peripherals, parts and accessories. Services will include the design, engineering, frequency coordination, installation, maintenance and repair of two-way radio network and microwave systems. The products and services include two-way radio subscriber units and fixed station equipment, including dual mode (analog and P25 digital), and accessories; microwave systems, components and accessories; trunking and conventional two-way radio systems, components, accessories and infrastructure; analog and P25 digital two-way radio systems and infrastructure; marine and amateur radios and accessories; fixed mobile data and automatic vehicle location (AVL) systems; public safety paging systems; radio dispatch console systems, related components and accessories; radio dispatch console furniture and related components; desktop radio remote systems and related components; radio gateway systems (analog and digital) and related accessories; Land Mobile Radio (LMR) antenna system components; category associated software updates, and not limited to the items identified. Services and/or repairs of any or all of the above listed items. (Excluded from this contract: Public Safety Broadband and LTE only communications equipment and services).

Product Specifications, including Environmental Standards and Requirements

Selection of EPP Equipment – The contract provides equipment that represents environmentally preferable products wherever possible. Such Equipment may use alternative fuel (e.g., compressed natural gas), offer an opportunity for reduced fuel usage, or provide other environmental benefits.

Technical Support

Where technical support response is included, Vendors shall supply at no charge, limited telephone technical support accessible toll-free, from at least 8 A.M. – 6 P.M., Monday through Friday for three (3) years after purchase. The maximum response time for technical support calls is four (4) hours from initial request to on-scene arrival unless otherwise agreed in writing between the Purchasing Entity and the Contractor. Bidders must include the costs, if any, for technical support calls in the Cost Tables.

Warranties/Repairs and Services

The warranty for the Commonwealth shall be the manufacturer's standard warranty starting from the date of acceptance by the Purchasing Entity. New equipment under this contract must be factory new and equipment considered a "durable commodity" shall carry a guarantee that service, service parts and maintenance will be available from the Contractor for a period of at least five (5) years from date of equipment acceptance by the Purchasing Entity. All equipment shall be in excellent working condition and shall include the new OEM equipment guarantee.

Other Discounts

- **Prompt Pay Discounts:** A discount given to the buyer if paid within a certain time period. These discounts may be found in the Vendor List and Information section below. All discounts offered will be taken in cases where the payment issue date is within the specified number of days listed by vendor 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.
- **Volume Discounts:** A discount is provided to buyer if a certain volume of product or service is purchased.
- **Dock Delivery Discount:** A discount is provided if product is delivered directly to the loading dock

If the Needed Product Can Not be Found

If a product or service cannot be found in the vendor's catalog, price sheet or PunchOut, it is recommended to contact the vendor directly to inquire if it is available for purchase on this contract. If the product or service meets the scope of the product category, the vendor may be able to add it to their product offerings with prior approval to add from the OSD contract manager.

If the product is not listed in the scope of the product category, a buyer may contact the Strategic Sourcing Lead to inquire whether the product may be purchased.

Performance and Payment Time Frames Which Exceed Contract Duration

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 written agreement shall extend more than twelve (12) months beyond the current contract term of this Statewide Contract as stated on the first page of this contract user guide. No new leases, rentals, maintenance, or other agreements for services may be executed after the Contract has expired.

Memorandum of Understanding/Statement of Work

Contract users must complete a detailed Statement of Work for any service engagement to be completed under this contract. The SOW template can be found under the "Attachment" tab in COMMBUYS under the PSE01 Master Blanket MBPO; it is recommended that Buyers use this format to request the following list and any other information as required by the engaging entity:

- Scope of Services/Deliverables Dates & Location of Service
- Detailed Budget
- Estimated Total Costs
- # Of Staff/Rate(s) Per Hour

Required Documentation from Contractor:

- Vendors are required to submit completed payment vouchers, and all required signed documentation to the designated Buyer personnel for processing. Vendors are obligated to pay prevailing wage rates to their employees who work in Commonwealth owned or rented facilities under this contract. Please report any known or suspected underpayment or non-payment of the prevailing wage to OSD for referral to the Attorney General's Office and the Department of Labor and Workforce Development. There is no Commonwealth form to report weekly janitorial prevailing wage, as there is for construction.

For non-Commonwealth owned or rented facilities, invoices for services rendered during the previous month must be submitted to the hiring entity according to the terms of the Statement of Work.

Strategic Sourcing Team Members:

SST Member Names	Agency
Thompson Clark, Kelly	OSD
Santana, NIkki	OSD
Billings, Daniel (Inactive)	OSD
Rostamnezhad, Reann	OSD
Walrath, Julie	DFS Fiscal
FitzGerald, Nancy	DFS Fiscal
Thomas, Al	DFS HAZMAT
O'Neil, Bryan	DFS MFA
Shipman, Peter	DFS Facilities
Daggett, Paula	DOC
Griffiths, Nolan	DOC
Dailey, Matthew	DOC
Coates, James	DOC
Griffin, James	DOC
Kearnan, Brian	MSP
Meagher, Ann	MSP
Fernandes, Paul	MSP
Gutowski, Gary	MSP

Barstow, Matt	MSP
Reardon, John	MEP
Wong, Robert	MEP
Rogers, Sharon	Barnstable Sheriff's Office
Urato, Tina	MEMA
Bagdonas, Andy	MEMA
Mahoney, Stephen	MassDEP Marine
Wilder, Scott	Brookline PD
Fitzgerald, Ken	Foxborough PD
Verdone, Robert	SEMRECC
Floyd, Erica	Springfield FD

Vendor List and Information*

Vendor	Master Blanket Purchase Order #	Contact Person	Phone #	Email	Categories	Discounts (PPD, Dock Delivery, Other)	SDO Certification Type	SDP Commitment Percentage
**[Master Contract Record] [Master MBPO] (All contract documents)	PO-22-1080-OSD03-SRC3-24063	Kelly Thompson Clark	617-720-3184	Kelly.ThompsonClark@mass.gov	N/A	N/A	N/A	N/A
***[Solicitation Enabled MBPO] (for requesting quotes) Category 1: Fire Public Safety Equipment and Two-Way Radios	PO-22-1080-OSD03-SRC3-24071	Kelly Thompson Clark	617-720-3184	Kelly.ThompsonClark@mass.gov	N/A	N/A	N/A	N/A
***[Solicitation Enabled MBPO] (for requesting quotes) Category 2: EMS Public Safety Equipment and Two-Way Radios	PO-22-1080-OSD03-SRC3-24070	Kelly Thompson Clark	617-720-3184	Kelly.ThompsonClark@mass.gov	N/A	N/A	N/A	N/A
***[Solicitation Enabled MBPO] (for requesting quotes) Category 3: Police Public Safety Equipment and Two-Way Radios	PO-22-1080-OSD03-SRC3-24061	Kelly Thompson Clark	617-720-3184	Kelly.ThompsonClark@mass.gov	N/A	N/A	N/A	N/A
***[Solicitation Enabled MBPO] (for requesting quotes) Category 4: Marine Public Safety Equipment and Two-Way Radios	PO-22-1080-OSD03-SRC3-24067	Kelly Thompson Clark	617-720-3184	Kelly.ThompsonClark@mass.gov	N/A	N/A	N/A	N/A
***[Solicitation Enabled MBPO] (for requesting quotes) Category 5: Two Way Radio Public Safety Equipment and Two-Way Radios	PO-22-1080-OSD03-SRC3-24068	Kelly Thompson Clark	617-720-3184	Kelly.ThompsonClark@mass.gov	N/A	N/A	N/A	N/A
Adamson Industries Corp.	PO-21-1080-OSD03-SRC04-24056	Steve Contarino	978-681-0370	scontarino@adamsonindustries.com	1,2,3,4	PPD: 1% - 10 days VPD: 2% (Greater than $25K) DDD: 2%	WBE	1.00%
Airgas Inc	PO-22-1080-OSD03-SRC3-24259	Naomi Albright	855-625-5285 Ext 4805	naomi.albright@airgas.com	1,2,3,4	PPD: 1% - 10 days		1.00%
ALL SPORTS HEROES UNIFORMS	PO-21-1080-OSD03-SRC04-24046	Mike McAtamney	978-452-1976 Ext 313	mmcatamney@allsportsheroes.com	3,5	PPD: 2% - 10 days 1% - 15 days .5% - 20 Days	WBE	1.00%
All-Comm Technologies	PO-21-1080-OSD03-SRC04-24049	Paul Boudreau	781-289-3000	pboudreau@allcomm1.com	5	PPD: 2% - 10 days 1% - 15 days to 30 days		2.00%

Vendor	Master Blanket Purchase Order #	Contact Person	Phone #	Email	Categories	Discounts (PPD, Dock Delivery, Other)	SDO Certification Type	SDP Commitment Percentage
Applied Communications Services Inc	PO-21-1080-OSD03-SRC04-24033	Stefan Georgules	508-393-9312	sgeorgules@appliedcomm.com	5	PPD: 2% - 10 days 1% - 15 days		1.00%
Atlantic Tactical	PO-21-1080-OSD03-SRC04-24015	Paul Newsham	978-505-4714	Paul.Newsham@atlantictactical.com	1,2,3,4,5	PPD: 1% - 10 days VPD: 2%		1.00%
AVIAT U.S., INC	PO-21-1080-OSD03-SRC04-24032	Bob Brown	603-479-2171	Bob.Brown@Aviatnet.com	5	N/A		1.00%
Axon Enterprise	PO-22-1080-OSD03-SRC3-28129	Vince Valentine	847-975-4834	vvalentine@axon.com	3	VPD: 10% (QTY 1-250) 20% (QTY 251 – 500) 30% (QTY 501 - 1,000)		5.00%
Ayacht Technology Solutions	PO-21-1080-OSD03-SRC04-24042	Mark Ayotte	978-558-0160	mayotte.commpass@ayacht.com	1,2,3,4,5	PPD: 1% - 10 days .5% - 15 days .3% - 15 days VPD: 2%		4.50%
B & B Engineering	PO-21-1080-OSD03-SRC04-24057	Daniel Dinwiddle	978-352-6660	ddinwiddle@lwbills.com	1.3	PPD: 2% - 10 days VPD: 5%		1.00%
Beltronics	PO-21-1080-OSD03-SRC04-24021	Bernard Peabody	603-402-4144 Ext 106	bernie@beltronics.net	5	PPD: 2% - 10 days 1% - 15 days VPD: 2%		1.00%
Bergeron Protective Clothing	PO-21-1080-OSD03-SRC04-24054	Richard Hillsgrove	603-496-0196	Rich@BergeronProtectiveClothing.com	1,2,3	PPD: 1% - 10 days VPD: 40%		1.00%
Blue Collar Customs, LLC	PO-22-1080-OSD03-SRC3-26935	Kyle Fonseca	781-421-6381	Kyle@BlueCollarCustomsMA.com	1 3	PPD: 1% - 10 days		1.00%
Body Armor Outlet	PO-21-1080-OSD03-SRC04-24014	Ray Bellia	603-327-8186	ray@bodyarmoroutlet.com	1,2,3	PPD: .5% - 10 days VPD: .25% - 15 days		1.00%
Brand Company	PO-21-1080-OSD03-SRC04-24020	Frank Twiss	978-468-4877	ftwiss@brandcompany.com	1,2,3,5	PPD:3% - 10 days 2% - 15 days 1% - 20 Days		1.00%
Brigham Industries	PO-21-1080-OSD03-SRC04-24050	Janice Bagdis	508-795-7905	jbagdis@brighamindustries.com	1,2,3,4	PPD: 2% - 10 days VPD: 5%	WBE	3.50%
C & S Specialty Inc	PO-22-1080-OSD03-SRC3-26936	Henry Heroux	401-769-2260	info@csspecialty.com	1 3	PPD: 2% - 10 days 2% - 15 days		1.00%

Vendor	Master Blanket Purchase Order #	Contact Person	Phone #	Email	Categories	Discounts (PPD, Dock Delivery, Other)	SDO Certification Type	SDP Commitment Percentage
						1% - 20 days		
Camelot Tools	PO-21-1080-OSD03-SRC04-24036	Lauren Cacela	508-981-7443	tools@camelottools.com	1,2,3	PPD: 5% - 10 days		2.00%
Central Equipment Co., LLC	PO-22-1080-OSD03-SRC3-26844	Jean Cole	(508)758-3758	jeanc@central-equipment.net	1 2 3 4 5	PPD: 1% - 10 days		1.00%
Central Lake Armor Express (Armor Express)	PO-22-1080-OSD03-SRC3-24198	Donna Corbin	231-350-6270	Dcorbin@armorexpress.com	3	PPD:2% - 10 days 1% - 15 days .5% - 20 days		1.00%
Colonial Ford	PO-21-1080-OSD03-SRC04-24026	John Welch	774-283-6400	jwelch@buycmg.com	1,2,3,4	PPD:1% - 10 days .5% - 15 days VPD: 1% DDD: 1.5%		1.00%
Common Cents EMS Supply LLC	PO-22-1080-OSD03-SRC3-26984	Joseph Johnson	860-388-4599	joe@savelives.com	1 2 3	PPD: 1% - 10 days		1.00%
Comtronics - A Bearcom Company	PO-22-1080-OSD03-SRC3-24164	Lynn Chandler	617-770-0212	lynn.chandler@bearcom.com	5	PPD: 2% - 10 days 1.5% - 15 days 1.5% - 15 days VPD: 2%		2.00%
Connecticut Radio	PO-21-1080-OSD03-SRC04-24031	DJ Bighinatti	860-563-4867	dj@connradio.com	5	PPD: 5% - 10 days 3% - 15 days VPD: 3%		10.00%
Cyber Communications	PO-21-1080-OSD03-SRC04-24045	John Connolly	781-647-1010	jconnolly@cybercomminc.com	5	PPD: 2% - 10 days 1% - 15 days .5% - 15 days VPD: 2%		1.50%
D&R COMMUNICATIONS	PO-21-1080-OSD03-SRC04-24018	Roger B Santerre	508-943-9595	rbs@drradio.com	5	PPD: 2% - 10 days 1% - 15 days VPD: 30%		1.00%
East Coast Emergency Outfitter	PO-22-1080-OSD03-SRC3-24244	Brian Lindsay	866-639-0279	brian@emergencyoutfitter.net	1,2,3	PPD: 2% - 10 days VPD: 2%		1.00%

Vendor	Master Blanket Purchase Order #	Contact Person	Phone #	Email	Categories	Discounts (PPD, Dock Delivery, Other)	SDO Certification Type	SDP Commitment Percentage
EASTERN COMMUNICATIONS LTD	PO-21-1080-OSD03-SRC04-24027	Gregg Moshensky	718-729-2044 Ext 322	gsm@easterncommunications.com	5	PPD:.4% - 10 days .3% - 15 days .2% - 20 Days		1.00%
Elmridge Protection Products, LLC	PO-22-1080-OSD03-SRC3-26985	Jonathan Tyfield	561-244 8337	admin@elmridgeprotection.com	1	PPD: 0.1% - 10 days		1.00%
ErgoFlex Systems, Inc. dba Xybix Systems, Inc.	PO-22-1080-OSD03-SRC3-26934	Kenneth Carson	303-683-5656	KenC@xybix.com	1 2 3 5	PPD: 0.5% - 10 days 0.1% - 15 days		1.00%
Fire Equipment	PO-21-1080-OSD03-SRC04-24060	Joe Golini	781-827-5119	jgolini@feinewengland.com	1	PPD: 1% - 10 days		1.00%
Fire Tech and Safety of New England	PO-21-1080-OSD03-SRC04-24053	Matthew Wicks	978-649-6800	Mwicks@firetechusa.com	1,2,3,4	PPD: 3% - 10 days 2% - 15 days 1% - 20 Days VPD: 5%		1.00%
FIREMATIC SUPPLY	PO-21-1080-OSD03-SRC04-24019	Matt Dube	978-514-4099	mdube@firematic.com	1,2,3,4	PPD: 1% - 10 days		1.00%
Galls LLC	PO-21-1080-OSD03-SRC04-24016	Amelia Smeltzer	859-800-1400	smeltzer-amelia@galls.com	1,2,3	PPD: 1% - 10 days		1.00%
Global Public Safety	PO-21-1080-OSD03-SRC04-24038	Joshua Bassett	603-309-4058	joshua.bassett@globalpublicsafety.us	1,2,3	PPD: 1% - 10 days .5% - 15 days DDD: 2%		100.00%
GOOSETOWN ENTERPRISES, INC.	PO-21-1080-OSD03-SRC04-24022	Todd Stacy	860-528-7500 Ext 323	tstacy@goosetown.com	1,2,3,4,5	PPD: 3% - 10 days 1.5% - 15 days .5% - 20 Days VPD: 1% DDD: 1%		2.00%
Green Mountain Communications	PO-21-1080-OSD03-SRC04-24058	Heather Hagar Robert Covino	603-717-7117 Ext 22	Accounts.payable@greenmtncomm.com Robert.Covino@greenmtncomm.com	5	PPD: .5% - 10 days .3% - 15 days .1% - 20 Days		1.00%

Vendor	Master Blanket Purchase Order #	Contact Person	Phone #	Email	Categories	Discounts (PPD, Dock Delivery, Other)	SDO Certification Type	SDP Commitment Percentage
Guardian Uniform and Supply	PO-21-1080-OSD03-SRC04-24044	Theresa Goodrich	413-858-8880	Terry@guardianuniform.com	1,2,3,4,5	PPD: .5% - 10 days		1.00%
Harrison Shrader Enterprises LLC	PO-22-1080-OSD03-SRC3-27103	Bill Shrader	(207) 312-4991	bill@hsefiresafety.com	1 2 3 4	PPD: 2% - 10 days		1.00%
Horizon Technologies Inc	PO-21-1080-OSD03-SRC04-24041	Dan Ouellette	928-763-4433	douellette@horizontechnologies.us	5	PPD: 5% - 10 days 4% - 15 days 3% - 20 Days 2% - 30 Days VPD: 4%		3.00%
Industrial Communications	PO-21-1080-OSD03-SRC04-24048	Melissa Goodwin	781-319-1087	melissa.goodwin@induscom.com	5	PPD: 2% - 10 days 1% - 15 days		3.00%
Industrial Protection Services	PO-21-1080-OSD03-SRC04-24043	Kevin Murphy	603-685-8040	kmurphy@ipp-ips.com	1,2,3,4	PPD: 1% - 10 days		2.00%
Island Tech Services	PO-21-1080-OSD03-SRC04-24029	Robert Gronenthal	888-615-2770 Ext 236	robert@itsg.us.com	1,3	PPD: 2% - 10 days 1.5% - 15 days 1% - 20 Days		1.00%
JUREK BROTHERS	PO-21-1080-OSD03-SRC04-24047	Greg or Nick Jurek	413-774-2783	sales@jurekbrothers.com	1,2,3,4	PPD: 1% - 10 days .8% - 15 days .5% - 20 Days		1.00%
Keane Fire & Safety Equipment	PO-21-1080-OSD03-SRC04-24023	Beth Hayes	781-899-6565 Ext 113	bhayes@keanefire.com	1	PPD: 2% - 10 days	WBE	10.00%
KMW Hardware Inc dba A C & M Fire Equipment	PO-21-1080-OSD03-SRC04-24037	Kevin Whalen	978-264-4412 Ext 102	kevin@acmfireequipment.com	1	PPD: 2% - 10 days 1.5% - 15 days 1% - 20 Days VPD: 3% (Qty 15 or greater)		1.00%
Kustom Signals, Inc.	PO-22-1080-OSD03-SRC3-27102	Jim Lindquist	913.492.1400	jlindquist@kustomsignals.com	3	VPD: 5% (QTY 100)		1.00%
L3Harris Technologies	PO-21-1080-OSD03-SRC04-24055	Ed Muller	603-275-0877	Ed.Muller@L3Harris.com	3,4,5	PPD: 1% - 10 days VPD: 31%		1.00%

Vendor	Master Blanket Purchase Order #	Contact Person	Phone #	Email	Categories	Discounts (PPD, Dock Delivery, Other)	SDO Certification Type	SDP Commitment Percentage
MAG Retail Holdings FFD	PO-22-1080-OSD03-SRC3-24199	Clay Chase	508-494-6699	cchase@mcgovernauto.com	1,2,3,4	PPD: 1% - 10 days		1.00%
Marcus Communications	PO-21-1080-OSD03-SRC04-24025	Michael Bula	800-833-7724	mike@marcusradio.com	5	PPD: 2% - 10 days 1% - 15 days 1% - 20 days		1.00%
Mirion Technologies (Canberra), Inc.	PO-22-1080-OSD03-SRC3-27104	Patrick McElroy	203-631-2558	pmcelroy@mirion.com	1, 2, 3, 4	VPD: 2.5 % (QTY 101-500)		1.0%
Modular Communications	PO-21-1080-OSD03-SRC04-24040	Lee Lemoine	603-203-5774	lee.lemoine@modularcommunications.com	5	PPD: 2% - 10 days 1.5% - 15 days 1% - 20 days VPD: 2% DDD: 1%		3.00%
Motorola Solutions, Inc.	PO-22-1080-OSD03-SRC3-25116	Mike Sheridan	508-797-2233	msheridan@motorolasolutions.com	3, 5	N/A		5.00%
Neptune Uniforms & Equipment, Inc.	PO-22-1080-OSD03-SRC3-26933	Linda Tobin	978-372-8812 X120	ltobin@neptuneuniforms.com	1 2 3	PPD: 4% - 10 days 3% - 15 days 2% - 20 days 1% - 30 days VPD: 3%		1.00%
New England Fire Equipment & Apparatus Corporation	PO-22-1080-OSD03-SRC3-26843	Randy Crowe	401-481-8999	Rcrowe@nefea.com	1 2 3	PPD: 2% - 10 days VPD: 2%		1.00%
NEWCOM Wireless Services, LLC	PO-21-1080-OSD03-SRC04-24028	Dov Koplovsky	781-826-7989	dov.koplovsky@newcomglobal.com	1,2,3,4,5	PPD: 2% - 30 days		51.00%
Northeast Rescue Systems Inc	PO-21-1080-OSD03-SRC04-24052	Dorothy Oconnor	617-325-3993	info@northeastrescue.com	1,2,3,4,5	PPD: .5% - 10 days	WBE	1.00%
Northeast Two-Way Radio Corp	PO-21-1080-OSD03-SRC04-24017	Jason Martocchio	978-532-1160	jason@northeastradios.com	1,3,5	PPD: 2% - 10 days 1.5% - 15 days 1% - 20 days		1.50%
Pittsfield Communications Systems	PO-21-1080-OSD03-SRC04-24059	Shannon Ullrich	413-448-8214	sullrich@pittsfieldcommunications.com	5	PPD: 2% - 10 days 1.5% - 15 days 1% - 20 days		2.00%

Vendor	Master Blanket Purchase Order #	Contact Person	Phone #	Email	Categories	Discounts (PPD, Dock Delivery, Other)	SDO Certification Type	SDP Commitment Percentage
PURVIS Systems Incorporated	PO-21-1080-OSD03-SRC04-24024	Mr. Rick Foster	401-619-2469	rfoster@purvis.com	1,2	PPD:3% - 10 days 2% - 15 days 1% - 20 days .5% - 30 days		5.00%
RDC Communications, Inc.	PO-21-1080-OSD03-SRC04-24034	Dale Boisvert	508-394-2405	dale@capeelectronics.com	5	PPD: 1.5% - 10 days 1% - 15 days .5% - 20 days VPD: 3%		1.00%
Strategic Safety Dynamics, LLC	PO-21-1080-OSD03-SRC04-24039	Joseph Beltrani	631-724-2646	info@ssdonline.us	1,2,3	PPD: 1% - 10 days VPD: 5%		5.00%
TCS Communications Corp.	PO-21-1080-OSD03-SRC04-24051	Todd Williams	978-465-7932	todd.williams@tcscommunications.com	5	PPD: 2% - 10 days 1.5% - 15 days 1% - 20 days VPD: 2%		2.00%
TESSCO Incorporated	PO-21-1080-OSD03-SRC04-24035	Rommel Marcelino	410-773-3576	marcelinor@tessco.com	5	PPD: 2% - 10 days		1.00%
Triple P Enterprises, Inc. dba Doughboy Uniforms	PO-22-1080-OSD03-SRC3-26986	Paul Simonini	781-284-6000	psimonini@DoughboyRevere.com	1,2,3	N/A		2.00%
Zetron, Inc.	PO-21-1080-OSD03-SRC04-24030	Tiffany Carey	425-820-6363	tcarey@zetron.com	5	VPD: 5%		1.00%
ZOLL Medical Corporation	PO-22-1080-OSD03-SRC3-26842	Stacy Freeman	351-500-3500	stacy.freeman@zoll.com	1 2 3 4	PPD: 1% - 10 days		3.70%

*Note that COMMBUYS is the official system of record for vendor contact information.
**[The Master Contract Record MBPO is the central repository for all common contract files. Price files may be found in the individual vendor's MBPO.
*** The Solicitation Enabled MBPO is for multiple quote requests and price comparison.

Appendix A:

UNSPSC Codes for PSE01

Fire:

26-12-16: Electrical cable and accessories
31-15-15: Roped
31-15-16: Chains
31-15-17: Mechanical Cable
31-15-18: Mechanical Wire
31-15-19: Straps
31-15-20: Security Wire
31-15-21: Cords
31-15-22: Nonelectric iron and steel wire
31-15-23: Nonelectric nonferrous metal wire
31-18-17: Packings and glands
31-18-18: Automotive boots and covers
31-20-15: Tape
31-20-16: Other Adhesives and Sealants
31-21-15: Paints and Primers
31-21-16: Paint Additives

31-21-17: Miscellaneous Finishes
31-21-18: Paint solvents and thinners
31-21-19: Paint applicators and painting accessories
39-11-20: Portable and Temporary Lighting and accessories
46-16-17: Rescue equipment and accessories
46-18-15: Safety apparel
46-18-16: Safety footwear
46-18-17: Face and head protection
46-18-18: Vision protection and accessories
46-18-19: Hearing protectors
46-18-20: Respiratory protection
46-18-21: Anti-static equipment and supplies
46-18-22: Ergonomic support aids
46-18-23: Fall protection and rescue equipment
46-18-24: Decontamination aids and safety cleaning equipment
46-18-25: Personal safety devices or weapons
46-19-15: Fire prevention
46-19-16: Fire-fighting equipment

EMS:

42-17-15: Emergency medical services disaster management products
42-17-16: Emergency medical services extricating and immobilizing and transporting products

42-17-17: Emergency medical services blankets
42-17-18: Emergency medical services airway management equipment
42-17-19: Emergency medical services storage cases and bags
42-17-20: Emergency and field medical services kits
42-17-21: Emergency medical services resuscitation products
42-17-22: Emergency medical services supplies
42-18-16: Blood pressure units and related products
42-18-18: Pulse oximeters
42-18-21: Stethoscopes and related products
42-18-22: Medical thermometers and accessories
42-18-26: Medical exam lights or lamps
42-27-17: Oxygen therapy delivery systems and devices
42-27-19: Airway management products
42-27-20: Intubation supplies
42-30-15: Aids for medical training
42-31-15: Bandages and dressings and related products

Police:

12-14-20-05: Helium gas He
15-11-15-06: Acetylene
46-15-15: Crowd control equipment
46-15-16: Security and control equipment

46-15-17: Forensic equipment and supplies and accessories
46-15-18: Explosives control equipment and accessories and supplies
46-15-19: Chemical biological control equipment and accessories and supplies
46-16-15: Traffic control
46-17-15: Locks and security hardware and accessories
46-17-16: Surveillance and detection equipment
46-20-10: Public safety training equipment
46-20-11: Small arms weapons training equipment
78-11-15: Passenger air transportation

Marine:

25-11-19: Marine craft systems and subassemblies
46-16-16: Water safety
49-14-15: Scuba and snorkeling gear
49-14-16: Surf and swim equipment and accessories

Two-Way Radio:

32-10-15: Circuit assemblies and radio frequency RF components
43-19-15: Personal Communication Devices
43-19-16: Personal Communication Devices Accessories & Parts
43-22-17: Fixed Network Equipment & Components
81-11-18: Two Way Radio Maintenance & Support Services

83-11-16: Mobile communications services
83-11-19: Radio services
83-11-22: Enhanced telecommunications services
83-11-23: Fiber telecommunications services
83-11-24: Switched dial up and leased dedicated line circuit telecommunications services

MOTOROLA SOLUTIONS

3109







MASSACHUSETTS PORT AUTHORITY

MassPort/MSP-Cruisers 24 M500 and WiFi Base

04/21/2023

The design, technical, pricing, and other information (" Information ") furnished with this submission is confidential proprietary information of Motorola Solutions, Inc or the Motorola Solutions entity providing this quote (" Motorola ") and is submitted with the restriction that it is to be used for evaluation purposes only To the fullest extent allowed by applicable law, the Information is not to be disclosed publicly or in any manner to anyone other than those required to evaluate the Information without the express written permission of Motorola
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

Massachusetts Department of State Police
Automated License Plate Recognition (ALPR) System
Memorandum of Understanding and Agreement

THIS AGREEMENT, made and entered into this _31_____ day of __May_____, 2022 by and between the Department of State Police, hereinafter referred to as "Department," and the

___Raynham 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.

Colonel Christopher S. Mason
Massachusetts State Police

2-13-20
Date

Representative:
Agency:

05/31/2022
Date

3115

MA State Police
READS REPORT

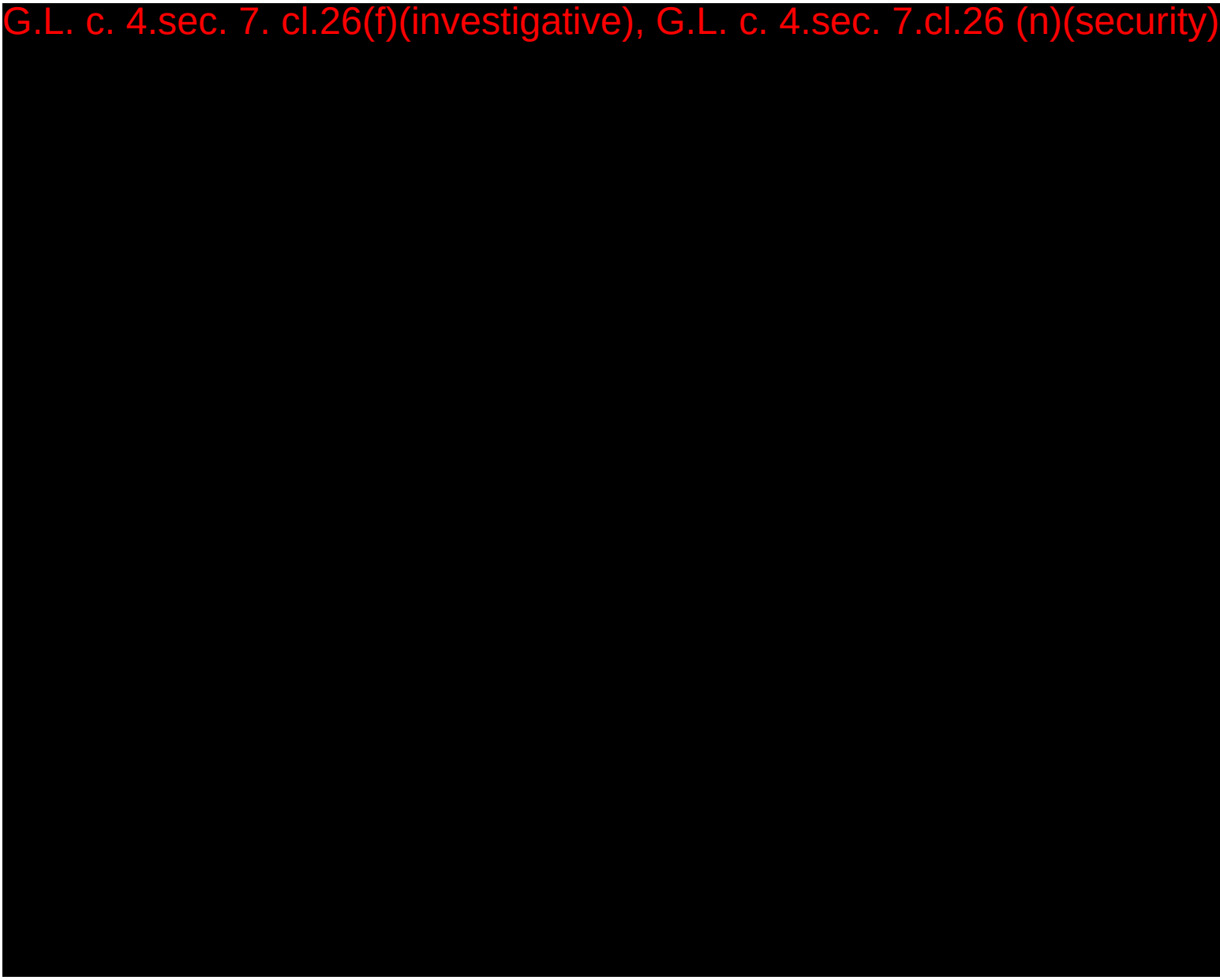
boss4

Creation Date: 05/29/2023 08:24
User: Sean Bender
From: 05/16/2023 00:00
To: 05/29/2023 08:24
Timezone: Eastern Time (US & Canada)

Hits
Misreads

LICENSE PLATE	PATCH	VEHICLE	TIMESTAMP	ADDRESS

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





BOSS4

Features & Improvements

Release Notes

Version 59.0.0

Permission by device

- Device permissions per groups – Configuration in groups to select active devices. The device management phase from the Devices screen is pending.
- Reports permissions per group.
- Filters only return devices selected in the group.

Auto-notification of hotlist and hot plate expiration

- Hotlist with manual hotplates will send an email with the expiration date of the hotlist and a PDF file with the hotplates that are near to expire.
- Hotlist with a hotsource will send an email with the expiration date of the hotlist.
- Reports- Decommissioned devices are returned when creating reports.
- Search- The device's full name is displayed using a tooltip.
- Vehicular traveling- Change the remaining text suspicious travel to vehicular traveling.
- Reads Report- Increase image size in report.
- VES-HUB validation- Control malformed events added to the VES MS.
- VES-HUB – Java upgrade 8 to 11 improving memory usage.
- Reports - When a user selects schedule report and selects 1 day the report will return the results of the previous 1-day calendar.

Fixes

- Fixed an issue when entering blank spaces in the Plate text input cause the process to generate reports to fail.
- Fixed an issue where a Reads Report containing more than 2M record was failing due to a wrong pagination.
- Fixed an issue where the key file used for the exporter was incompatible with certain SFTP services.

Release Notes

Version 58.0.0

- Devices- Redux updated to return the device changes correctly. (The redux version was updated to improve the update of information between components and states within the validations of the elements)
- Search- Improvements in response times using wildcards. (A new index was added to database records to improve search times)
- Search - Fixed Day/Night mantis filters now return the correct results. (The query did not contemplate the times of the readings, so the times in which the readings return and additional information from mantis were delimited to readjust the query, returning the corresponding values of the search)
- Search - Fixed Search time & date filter overlap with the calendar button. (Autofit function was added, only the text is displayed depending on the size of the device where boss4 was opened)
- Search - Fixed Search time & date filter start/end times no longer allow typed-in times. (A component was sought that would allow the values to be modified while maintaining the new functionality of the historical limit.)
- Search - Fixed virtual scroll jumps in devices and user filters. (Simplified scroll element actions and integrated native behaviors for pre-loading elements)
- Reports- Read Detail Report the double negative was eliminated in NTP status. (Tag name change)
- Reports- Read Detail Report fixed image aspect ratio. (Depending on the number of bytes in the image, the size of the image to be used in the report is calculated without affecting the proportions of the vehicle.)
- Reports- Reads Statistics Report Improve in report creation to avoid failures.
- Reports- Reads Statistics by Device Improve report creation to avoid failures.
- Reports- Hits by Hotlist Report Improve in report creation to avoid failures.
- Reports- Hits by Hotlist by Device Report Improve report creation to avoid failures.
- Reports- Login Pagis Report Improve in report creation to avoid failures.

(The database is directly consumed avoiding the use of ms and avoiding stressing them, having better results in report generation, and avoiding timeouts)

- Notifications- New text box to search by profile name/ username. (A search box was integrated that returns the names of notification profiles and/or usernames within a profile, facilitating the search for a user or profile)
- Notifications- New functionality to visualize the complete hotlist when the user is above the name. (Angular's native tooltip was integrated to display long names)
- Notifications- Fixed notification sorting names with spaces at the beginning. (Front end deletes the spaces at the begging when the user creates/updates a notification profile)

- Notification- Fixed data from field 1 of the hit is repeated. (The same data was being consumed in all the fields; it was solved by specifying the correct data in each field)
- Interoperability- Fixed the option to send a sharing request between environments. (Error messages and connections messages were not the same in the databases, the information was adapted to be equal in databases and enable the connections between instances)
- Hotlist- Fixed arrows keep working no matter the zoom value. (The original size of the elements was lost, now the size is persisted adjusting the element depending on the zoom)
- Formatters- Now working with includes and excludes in the same formatter. (The algorithm was adjusted to add the logic to be able to use both configurations in the same formatter)
- Read/Hit detailed report improvement - the database was consulted directly to avoid timeouts and improve time-generating the report.

Release Notes

Version 57.0.2

- Search- Search pagination increased from 15 to 50 results.
- Search- New option to configure a user group to access only a certain amount of historical data i.e., 1 day, 30 days, etc.
- Search- New calendar control for setting the DateTime filters.
- Device Notifications- “No Reads Received” option added to alert when a device is not sending reads.
- Device Notifications- Screen layout improved.
- Reports- New layout for the Read and Hit Reports. Includes larger vehicle overview picture.
- Reports - Read and Hit Report - Feature to download the full overview picture as a JPG file.
- Notifications- Profile templates are now sorted by name.
- Desktop App- Include API GW Port to customize the connection to BOSS4.
- Search- Fixed duplicated hotlist field information.
- Search- Fixed a bug where some reads disappeared from the search screen when updated by a PAGIS device.
- PAGIS MS- Improve stability of microservice.
- PAGIS- Improved synchronization with PAGIS 2.14 and 2.15

For additional information, assistance please contact Neology ALPR/ANPR Support at:

Phone: (833-747-7577)

- Option 1 for Sales
- Option 2 For Support
- alpr_support@neology.net USA Support Teams Email.

For Customers in Europe, the Middle East, and Africa:

Sales Enquiry Email sales@uk.neology.net

Support Enquiry Email support@uk.neology.net

Web: https://neology.net

Corporate Office: 1917 Palomar Oaks Way, Suite 110, Carlsbad, CA 92008


VSLEA
VIGILANT SOLUTIONS LAW ENFORCEMENT ACADEMY
"Res Nostrae Elit"
CERTIFICATE OF TRAINING
THIS CERTIFICATE IS PROUDLY PRESENTED TO
Justin Salvatore
FOR THE SUCCESSFUL COMPLETION OF
VIGILANT VEHICLEMANAGER 101
on Jul 09, 2023
1 Hour
PRESENTED BY
Marcia Broderick
Marcia Broderick
Director, Customer Training and Development
MOTOROLA SOLUTIONS



CERTIFICATE OF TRAINING

THIS CERTIFICATE IS PROUDLY PRESENTED TO

Justin Salvatore

FOR THE SUCCESSFUL COMPLETION OF

VIGILANT VEHICLEMANAGER INTRODUCTION & USER ACCOUNT MANAGEMENT

on Jul 09, 2023
30 Minutes

PRESENTED BY

Marcia Broderick

Marcia Broderick
Director, Customer Training and Development

MOTOROLA SOLUTIONS

REKOR
INTELLIGENCE DRIVEN INNOVATION

Contract Number: <# <Content Select="//contract_number" TrackName="contract_number" Optional="true"/> #>

EQUIPMENT AND SOFTWARE MASTER SUBSCRIPTION AGREEMENT

This Equipment and Software Master Subscription Agreement (this "**Agreement**") is dated as of (the "**Execution Date**"), and is made by (i) Rekor Recognition Systems, Inc. ("**Rekor**"), with an address of 6721 Columbia Gateway Drive, Suite 400, Columbia, MD 21046 and (ii) <# <Content Select="//account_name" TrackName="account_name" Optional="true"/> #> ("**User**"), with an address of <# <Content Select="//billing_address" TrackName="billing_address" Optional="true"/> #>. Each of Rekor and User is referred to herein as a "**Party**" and collectively, the "**Parties**".

*Whereas, Rekor sells equipment (the "Equipment") and services (each a "Service" and collectively the "Services") as specified in each Schedule executed from time to time by Rekor and User in a form acceptable to Rekor (each a "**Schedule**" and collectively the "**Schedules**"). Each Schedule forms part of and is subject to this Agreement and all terms and conditions in this Agreement will apply to all Schedules.*

Whereas, User desires to engage Rekor to provide Equipment and related Services in accordance with the commercial specifications as noted in each Schedule and the terms of this Agreement.

Now, therefore, in consideration of, and conditioned on, the covenants, terms and conditions stated and incorporated herein, and for other good and valuable consideration, the receipt and sufficiency of which the Parties hereby acknowledge, the Parties agree as follows:

1. EQUIPMENT AND SOFTWARE

1.1. Equipment. The equipment listed and described in the Schedule attached hereto and incorporated herein.

1.2. Acceptance. User shall inspect each item of Equipment delivered or installed pursuant to the Agreement. User shall immediately notify the Rekor of any discrepancies between such item of Equipment and the description of the Equipment in the Schedule. If the User fails to provide such notice before accepting delivery of the Equipment, the User will be conclusively presumed to have accepted the Equipment as specified in the Schedule.

1.3. Installation of Equipment. Installation of the Equipment is available subject to a fee. If Rekor will perform the installation, User shall provide Rekor with access to the infrastructure necessary to facilitate the performance under this Agreement. This access includes, but is not limited to, power, network and internet connectivity and applicable regulatory permitting. Any cost for the initial power connection and monthly power service are the responsibility of the User. Services such as construction, engineering drawings, permits or other activities would incur an extra charge. With respect to the existing physical locations where the Equipment will be installed, User warrants possession of the right and sufficient authority to approve the installation of the Equipment.

1.4. Software License Grant. Rekor hereby grants to User, solely for User's own internal use, a non-transferable, non-assignable, non-exclusive license to use the software described herein (the "**Software**") and provided by Rekor to User. The User shall use the Software exclusively for the operation of the Equipment and shall not copy the Software in any form, whether in whole or in part, and shall not incorporate the Software, whether in whole or in part, or the Software's code, into any product for distribution or use by any third party. Except for the rights enumerated in the Agreement, the license hereby granted to User does not include a grant to User of any other rights to, title, ownership, security interest, or other interest, in any intellectual property of Rekor. The Software includes a collection of computer object code, documentation, precompiled binaries, and run time data used by the application code to analyze video stream data and perform various calculations and outputs.

1.5. Title to Software. The Software and all programs developed hereunder are proprietary to Rekor. Rekor shall retain exclusive right, ownership, title and interest in and to the Software, including all intellectual property rights. All applicable rights to patents, copyrights, trademarks and trade secrets in the Software or any modifications made at User's request are and shall remain in Rekor. User agrees to secure and protect each module, software product and documentation thereof in a manner consistent with the maintenance of Rekor's rights therein and to take appropriate action by instruction or agreement with its employees or consultants who are permitted access to each program or software product to satisfy its obligations hereunder. User agrees not to modify the software or create derivative products. Violation of any provision of this Section 1.5 shall be the basis for immediate termination of the Agreement.

1.6. Software Ownership. Rekor represents that it is the owner of the Software and all portions thereof and that it has the right to modify same and to grant User a license for its use.

1.7. Updates and Use. Rekor may provide User, from time to time, with updates (including minor adaptations, patches and bug fixes). User hereby warrants to keep the Software up-to-date and install all relevant updates. However, nothing in the Agreement shall require Rekor to provide updates, fixes or upgrades. User shall limit the use of the Software to its employees who have been appropriately trained.

1.8. Third Party Software. User acknowledges and agrees that the Rekor may use third party software with the Equipment. Such software may be subject to certain license agreements, regulations, conditions and terms established by such third parties in order to protect ownership and intellectual property rights in the software. The User acknowledges and agrees not to attempt to resell or redistribute such software.

2. WARRANTY

2.1. Rekor warrants that the Equipment and Software will conform, as to all substantial operational features, to Rekor's current published specifications when delivered or installed and will be free of defects which substantially affect system performance. The warranty is non-transferable.

2.2. **Software**. User must notify Rekor in writing, within 7 days of delivery of the Software to the User (not including delivery of any subsequent modifications to the Software), of its claim of

any such defect. If the Software is found defective by Rekor, Rekor's sole obligation under this warranty is to remedy such defect in a manner consistent with Rekor's regular business practices.

2.2.1. Modifications to the Software are strictly prohibited as is the creation of any derivative product. If any modifications are made to the Software by User during the warranty period, this warranty shall immediately be terminated. Correction for difficulties, defects or damages traceable to User's errors or systems changes shall be billed at Rekor's standard time and material charges.

2.2.2. User shall provide Rekor details regarding any bug, defect or failure in the Equipment or Software promptly and with no delay from such event. User shall also comply with Rekor's request for information regarding bugs, defects or failures and furnish with information and try to reproduce such bugs, defects or failures.

2.3 **Equipment**. The Equipment will be free from defects in material and workmanship and will conform and perform substantially in accordance with the documentation. The warranty period is:

2.3.1 Edge Pro: 3-years from the date of purchase.

2.3.2 Edge Max: 5-years from the date of purchase.

If, during the warranty period, the equipment does not conform to the above warranty and User provides Rekor with written notice of such nonconformance, Rekor will repair or replace nonconforming components or otherwise correct the nonconformity in accordance with its stated warranty service terms.

SUBJECT TO THE TERMS SPECIFIED IN THIS SECTION 2, THIS IS A LIMITED WARRANTY, AND SETS FORTH THE ONLY WARRANTIES MADE BY REKOR. NEITHER REKOR NOR ITS SUPPLIERS MAKE ANY OTHER WARRANTIES, CONDITIONS OR UNDERTAKINGS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. USER MAY HAVE OTHER STATUTORY RIGHTS. HOWEVER, TO THE FULL EXTENT PERMITTED BY LAW, THE DURATION OF STATUTORILY REQUIRED WARRANTIES, IF ANY, SHALL BE LIMITED TO THE WARRANTY PERIOD OR ANY APPLICABLE EXTENDED WARRANTY PERIOD

3. DATA RIGHTS.

The data, images, and video produced from using the Services is the "Operational Data." User retains all rights and ownership in your Operational Data, and we do not claim any ownership rights in your Operational Data. User grants Rekor the right and license to use the Operational Data for: a) dissemination to other government entities, and b) training and performance enhancement of Rekor's AI system. The data, images, and video produced from using the Services, where the license plate characters have been removed, is the "De-Identified Data". User acknowledges and agrees that Rekor may use the De-Identified Data for any purpose and may disclose the De-Identified Data to third parties. User must inform Rekor in writing before using the Services if the

laws of the jurisdiction in which you use the Services restrict the use of Operational Data or De-Identified Data for the purposes defined in this Section 3.

4. PAYMENT TERMS; TAXES

4.1. Payments. During the period in which the Agreement and each Schedule is effective, the User shall deliver to the Rekor payments of the amount and frequency set forth in the related Schedule (the "Payments"). The first Payment shall be due on the Effective Date. The Payments are due whether or not the User has received notice that a Payment is due.

4.2. Service Charge; Fees. If any payment is not paid within five (5) days after the due date, User shall pay to Rekor a service charge of 5% of the payment due per month which shall accrue each month until the outstanding balance is paid in full. User acknowledges that its ability to access the Services may require the payment of third-party fees and that User is responsible for paying such fees.

4.3. Collection Costs. If User fails to make any payments due under the Agreement and Rekor retains the services of a collection agency or an attorney to collect such amounts, User agrees to promptly pay to Rekor all reasonable costs of collection, including, but not limited to, any collection agency fees, reasonable attorney's fees, and court costs.

4.4. Tax. User shall pay all taxes, including any applicable sales or use tax, and all other fees or charges on or arising out of the Rekor's delivery of Services or Equipment to the User; however, the User will not pay any federal or state income taxes, franchise taxes, or any other taxes imposed on the Rekor's net income.

5. CONFIDENTIALITY

User agrees that it shall not disclose to any third party any information concerning the trade secrets, methods, processes or procedures or any other confidential, financial or business information of Rekor which should be reasonably understood to be confidential or non-public, whether or not such information is marked confidential, which User learns, directly or indirectly, or which is made available to User, as a result of this Agreement, without Rekor's prior written consent. User shall promptly notify Rekor in the event User becomes aware of any actual or purported loss or disclosure of any information covered by the prior sentence. If User is required by a legal or administrative process, including but not limited to, applicable law, regulation, order, or similar process, to disclose any information covered by the first sentence of this Section 5, User shall promptly notify Rekor of such requirement (if such notification can be made without violating the terms of such required disclosure), so that Rekor may seek an appropriate protective order or waive compliance with the Agreement. User agrees not to oppose any effort by Rekor to resist or narrow such requirement or to seek a protective order or other appropriate remedy. If, in the absence of a protective order or the receipt of a waiver hereunder, User is, in the opinion of its legal counsel, required to disclose such information, Recipient may disclose only such information to the party requiring disclosure as is required by law, regulation, order, or similar process. In connection with such required disclosure, User shall use its reasonable efforts, at Rekor's request and expense, to obtain from the party to whom disclosure is made written assurance that confidential treatment will be accorded to such portion of the information as is disclosed.

6. TERM; TERMINATION

6.1 Term: The term of the Agreement shall begin on the Effective Date, and unless earlier terminated in accordance with Section 6.2, shall continue until the latest expiration date of all Schedules in effect, (the "Term").

6.2 Default: The occurrence of any of the following shall constitute an event of default under the Agreement ("Event(s) of Default"):

6.2.1 The failure to make a required payment under the Agreement and each related Schedule when due.

6.2.2 The violation of any provision or requirement under the Agreement (other than making required payments) that is not corrected within ten (10) days after notice of the violation is given.

6.2.3 The insolvency of User.

6.2.4 The voluntary or involuntary commencement of a proceeding in bankruptcy or receivership against User or its property; a general assignment for the benefit of creditors by User or if User enter into an agreement or composition with its creditors; if User is dissolved or otherwise discontinued; or if User ceases doing business as a going concern.

6.2.5 The subjection of any of User's property to any levy, seizure, assignment, application or sale for or by any creditor or government agency.

6.2.6 The existence of any encumbrance on the Software that has not been approved by Rekor in writing.

6.2.7 If any application, certificate, statements, trade references, representations and/or financial reports furnished by User and submitted to Rekor proves to be false in any material respect.

6.3 Rights on Default: Upon the occurrence of any Event of Default, Rekor may, after any applicable cure period, without further notice to User, and in Rekor's sole discretion, exercise any one or more of the following remedies:

6.3.1 Declare User's obligations hereunder immediately due and payable and recover as liquidated damages and not as a penalty an amount equal to: (i) reasonable attorneys' fees; plus (any charges, costs, expenses, interest or penalties properly assessable against User pursuant to the provisions of the Agreement or any other agreement(s) between the parties;

6.3.2 Enforce performance by User of the applicable covenants and terms of the Agreement or recover damages for the breach thereof;

6.3.3 Terminate the Agreement and each related Schedule, terminate the licenses and take possession of the Software and associated documentation, with or without demand or

notice to User and without order of court or other legal process, and without incurring any liability to User for any damages incurred by reason of such taking; and/or

6.3.4 any other remedies available in law or at equity.

No failure or delay on the part of Rekor to exercise any remedy hereunder shall operate as a waiver. No express or implied waiver by Rekor of any default shall constitute a waiver of any other default by User or waiver of Rekor's rights. No remedy is intended to be exclusive, but each shall be cumulative and concurrent to the extent permitted by law and shall be in addition to any other remedy otherwise available to Rekor at law or in equity.

6.4 Effect of Termination. Expiration, termination or cancellation of the Agreement and related Schedules shall not affect rights, obligations or liabilities of the parties which accrue prior to such expiration, termination or cancellation. Upon expiration, termination or cancellation of the Agreement, all rights, licenses and authorizations granted to User hereunder will immediately terminate and User will (a) immediately cease all use of and other activities with respect to the Equipment and Software; (b) within 15 days deliver to Rekor all Equipment and Software at User's expense, or upon request by Rekor destroy the Software, and permanently erase from all devices and systems User directly or indirectly controls, the Software, including all documents, files, and tangible materials containing, reflecting, incorporating, or based on any of the foregoing, whether or not modified or merged into other materials; and (c) certify to Rekor in a signed written instrument that it has complied with the requirements of this Section 6.4. The provisions of Sections 3, 4.2 - 4.4, 5, 8.1-8.3, 8.6 and 8.7 of this Agreement shall survive termination of the Agreement and related Schedules.

7. COMMUNICATIONS AND REFERENCES.

Rekor and its subsidiaries (collectively, "**Rekor**") are each permitted to issue a press release announcing that User has retained Rekor to provide the Services. Rekor may reference User and generally describe the nature of the Agreement and its outcomes in Rekor's promotional materials, presentations, and proposals to current and prospective Users.

8. MISCELLANEOUS

8.1 Notices: All notices, requests, consents, claims, waivers and other communications (collectively, "Notices") hereunder shall be sent to the addresses set forth in the preamble of the Agreement and/or email set forth on the signature page to the Agreement or such other addresses and/or email as a Party gives from time to time. All Notices shall be deemed to have been given (a) when delivered by hand; (b) when received by the addressee if sent by a nationally recognized overnight courier (receipt requested); (c) on the date sent by facsimile or email, if sent during normal business hours of recipient, and on the next business day if sent after normal business hours of recipient or (d) on the third day after the date mailed, by certified or registered mail, return receipt requested, postage prepaid. All Notices hereunder may be given by any other means but shall not be deemed to have been duly given unless and until it is actually received by the intended recipient.

8.2 Entire Agreement and Modification: The Agreement (including the Schedules, Annexes and Exhibits hereto, and the provisions incorporated by reference herein) constitutes the entire agreement and understanding among the Parties hereto with respect to the subject matter hereof and supersedes all prior agreements and understandings, whether written or oral, relating to such subject matter in any way to the subject matter hereof or thereof. No modification, waiver or amendment of the Agreement shall be effective unless in writing and signed by both Parties. The Agreement replaces any and all prior agreements between the Parties with respect to its subject matter. Waiver by a Party of any provision of the Agreement does not constitute, and is not to be construed as constituting, a waiver of such provision (or any other provision) at any other time.

8.3 Governing Law. The Agreement shall be governed and construed in accordance with the laws of the State of Maryland, without application of any principle of Maryland law which would require that the Agreement be governed and construed by the laws of any other jurisdiction.

8.4 Log-In Information; Individual Use. To gain access to and use the Services, User may be required to create a username and password or other log-in ID and password ("Log-In Information"). User is responsible for all activity occurring under its Log-In Information, and User must keep its Log-In Information confidential and not share such Log-In Information with other individuals or third parties other than those with a business need to know. Rekor has no obligation or responsibility with regard to User's use, disclosure, or management of Log-In Information. Rekor may require User to change its Log-In Information if such Log-In Information is inconsistent with the terms of the Agreement. Notwithstanding anything set forth in the Agreement to the contrary, Rekor makes Services available to User for only its use and not for use by any third party.

8.5 Assignment, Sublease or Sublicense by User. User shall not assign, sublet or sublicense any interest in the Agreement, the Software, or permit the Software to be used by anyone other than User or User's employees, without Rekor's prior written consent. Any such assignment, sublet, or sublicense by User without the prior written consent of Rekor shall be null and void. Rekor in its sole discretion, reserves the right to assign this Agreement in parts or in its entirety.

8.6 Investigations. If Rekor becomes aware of any possible violations by User of any provision of the Agreement, Rekor reserves the right to investigate such violations. If, as a result of such investigation, Rekor believes that criminal activity has occurred, Rekor reserves the right to refer the matter to, and to cooperate with, any and all applicable law enforcement authorities. Except to the extent prohibited by applicable law, Rekor is entitled to disclose any information in Rekor's possession in connection with User's use of the Software, and under any provision of the Agreement, to (a) comply with applicable law, legal process or governmental request; (b) enforce the Agreement; (c) respond to any claims or rights of third parties; (d) respond to User's requests for customer services; or (e) protect the rights, property or personal safety of Rekor, its users or the public, and law enforcement or other government officials, as Rekor in its sole discretion believes to be necessary or appropriate. User is solely responsible for its familiarity and compliance with any laws that may prohibit User from participating in or using any part of the Services.

8.7 Submission to Jurisdiction; Consent to Service of Process; Waiver of Jury Trial. Each Party hereby irrevocably submits to the exclusive jurisdiction of the state and federal courts of the State of Maryland for the purposes of any suit, action or other proceeding arising out of or relating to the Agreement and agrees that all claims in respect of the suit, action or other proceeding may be heard and determined in any such court. Each Party agrees to commence any such suit, action

or other proceeding either in the state or federal courts of the State of Maryland. Each Party waives any defense of improper venue or inconvenient forum to the maintenance of any action or proceeding so brought and waives any board, surety or other security that might be required of any other party with respect thereto. Any Party may make service on any other Party by sending or delivering a copy of the process to the Party to be served in the manner provided for the giving of notices in Section 8.1. Nothing in this Section 8.7, however, shall affect the right of any Party to serve legal process in any other manner permitted by law or at equity. Each Party agrees that a final judgment in any action or proceeding so brought shall be conclusive and may be enforced by suit on the judgment or in any other manner provided by law or at equity. EACH OF THE PARTIES HEREBY IRREVOCABLY WAIVES ANY AND ALL RIGHTS TO TRIAL BY JURY IN ANY ACTION ARISING OUT OF OR RELATING TO THE AGREEMENT.

8.8 Severability. If any portion of the Agreement shall be held to be invalid or unenforceable for any reason, the remaining provisions shall continue to be valid and enforceable. If a court finds that any provision of the Agreement is invalid or unenforceable, but that by limiting such provision, it will become valid and enforceable, then such provision shall be deemed to be written, construed, and enforced as so limited.

8.9 Exhibits; Schedules. Except to the extent expressly modified by the Agreement, the Parties by their execution and delivery hereof, affirm and incorporate herein by reference all of the terms, covenants and conditions of the Exhibits, Schedules and terms and conditions expressly referenced herein as if such terms, covenants and conditions were fully set forth in the Agreement.

8.10 Relationship of the Parties. Rekor (and any affiliate thereof providing Services hereunder) is an independent contractor and service provider to User, and the Agreement shall not be deemed to establish a joint venture, partnership, association or fiduciary or similar relationship between Rekor or any affiliate thereof, on the one hand, and User or any affiliate thereof, on the other hand, for United States tax purposes or for any other purpose.

8.11 Further Assurances The Parties shall furnish upon request to each other further information, execute and deliver to each other documents, and do other acts and things, all as another party may reasonably request for the purpose of giving effect to the intent or express terms of the Agreement and the documents referred to in the Agreement; provided, that no party shall be obligated to incur any material liability, expense or obligation pursuant to this Section 8.11 without its consent.

8.12 Counterparts. The Agreement may be executed in counterparts, each of which is deemed an original, but all of which together is deemed to be one and the same agreement. A signed copy of the Agreement delivered by facsimile, e-mail or other mean of electronic transmission is deemed to have the same legal effect as delivery of an original signed copy of the Agreement.

[Signature Page Appears on Next Page]

IN WITNESS WHEREOF, the Parties have caused this Equipment and Software Master Subscription Agreement to be executed by their duly authorized representatives as of the Execution Date.

REKOR RECOGNITION SYSTEMS, INC.

By:_____

Printed name:_____

Title:_____

Email:_____

Phone:_____

USER:

By:_____

Printed name:_____

Title:_____

Email:_____

Phone:_____

REKOR
INTELLIGENCE DRIVEN INNOVATION

SCHEDULE

Schedule dated as of (the "**Schedule**") to Equipment and Software Master Subscription Agreement, effective as of , between Rekor Recognition Systems, Inc. ("**Rekor**") with an address of 6721 Columbia Gateway Drive, Suite 400, Columbia, MD 21046 and <# <Content Select="//account_name" TrackName="account_name" Optional="true"/> #> ("**User**"), with an address of <# <Content Select="//billing_address" TrackName="billing_address" Optional="true"/> #>, to be effective as of (the "**Effective Date**").

This Schedule is entered into pursuant to the Agreement. Except to the extent expressly modified hereby, the Parties hereto by their execution and delivery hereof, reaffirm and incorporate herein by reference all of the terms, covenants and conditions of said Agreement as if such terms, covenants and conditions were fully set forth in this Equipment and Software Subscription Schedule. All of the capitalized words used herein shall have the meanings ascribed to them in the Agreement unless otherwise expressly stated herein or therein.

1. Term: <# <Content Select="//term" TrackName="term" Optional="true"/> #>

2. Expiration Date: <# <Content Select="//expiration_date" TrackName="expiration_date" Optional="true"/> #>

3. Equipment Description: <# <Content Select="//equipment_description" TrackName="equipment_description" Optional="true"/> #>

4. Quantity of Systems: <# <Content Select="//quantity_of_systems" TrackName="quantity_of_systems" Optional="true"/> #>

5. Price: <# <Content Select="//annual_subscription_payment" TrackName="annual_subscription_payment" Optional="true"/> #>

6. Additional Notes/Conditions: <# <Content Select="//additional_notes_and_or_conditions" TrackName="additional_notes_and_or_conditions" Optional="true"/> #>

Counterparts. This Schedule may be executed in counterparts, each of which is deemed an original, but all of which together is deemed to be one and the same agreement. A signed copy of this Schedule delivered by facsimile, e-mail or other means of electronic transmission is deemed to have the same legal effect as delivery of an original signed copy of this Schedule.

[Signature Page Appears on Next Page]

IN WITNESS WHEREOF, the Parties have caused this Schedule to be executed by their duly authorized representatives as of the date first above written.

REKOR RECOGNITION SYSTEMS, INC.

By:_____

Printed name:_____

Title:_____

Email:_____

Phone:_____

USER:

_____

By:_____

Printed name:_____

Title:_____

Email:_____

Phone:_____

3136

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.macomptroller.org/forms. Forms are also posted at OSD Forms: https://www.mass.gov/lists/osd-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

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, _____ (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

SEARCH WARRANTS FOR DIGITAL STORAGE DEVICES & EVIDENCE

Presented By:

Jamie Michael Charles
Captain, Search Warrant Team

Chichi Lee
Assistant District Attorney, Search Warrant Team

MOSAIC THEORY FOR TECHNOLOGICAL SURVEILLANCE

- CW v. McCarthy, 484 Mass. 493 (2020) adopted the "mosaic theory"
- Advancing technology undercuts checks on overly pervasive police presence because:
  1) Not limited by same practical constraints
  2) Proceeds surreptitiously
  3) Gives LE access to info "previously unknowable"
- Recognizes privacy interest in whole of one's public movements

3141

ELSAG Mobile Plate Hunter MPH M7 ALPR System

Automatic License Plate Recognition



1: M7 Camera



Figure 2: Roof SUV Mounted M7 Camera



Figure 3: Trunk/Boot Mount M7 System

The new MPH M7 (7th generation) ALPR Camera System has a smaller trunkbox and thinner camera cables for easier and more compact installations of the High Definition 1280 x 1024 Cameras.

The product is suitable for:

- All vehicle makes and models.
- Compact design allows the ALPR/ANPR to fit in front of light bars on top of patrol cars or as a standalone unit attached by magnetic mounts. Unit is easily and rapidly transferable to a variety of police vehicles.
- Processor unit is the size of a small box for easy storage in trunk of a vehicle.
- The MPH M7 2 camera Number / License Plate Reader requires less than 20W of 12V DC (only about the draw of a car radio) to function.

The all-weather enclosure contains two cameras: a Black/White camera (with one IR illuminator) and one color overview camera. The B/W camera connected with an IR illuminator is designed to tackle variations of lighting conditions, from night to full sunlight.

For each plate read, the ELSAG Plate Hunter system provides:

- Black & white close-up photo of plate (from which the OCR Optical Character Recognition is done)
- Color overview photo of car and surrounding scene
- GPS Coordinates and mapping to show location that the plate was scanned
- Time and Date stamp

Elsag is a ALPR product of Selex ES, Inc. a Leonardo Company

Factory and Hardware Engineering
4221 Tudor Lane
Greensboro, NC 27410 USA
Tel +1 877 773 5724
Fax + 1 336 379 7164

Software Development Office
7 Sutton Place
Brewster, New York 10509 USA
Tel +1 845 278 5425

MPH M7 Camera Specifications

Figure 4: M7 Camera Views



M7 CAMERA SYSTEM SPECIFICATIONS	
B/W CAMERA	1280 x 1024 Monochrome CMOS Sensor (1/1.8")
Color Camera	1280 x 1024 Color CMOS Sensor (1/1.8")
Optics Interface	C Mount B&W, S Mount Color
IR Illumination	740nm LED illuminator synchronized with camera shutter, (870nm optional)
Camera Interface	Proprietary 8 pin Military grade connector IP67 rated
Camera Communication Protocol	LVDS Digital Interface
Optics	25mm, 16mm, 12mm 8mm (Black/White reading camera)
Operating Temperature	-40 – +60'C (-40 – +140'F)
Housing Protection	IP67
Operating Humidity	10-90% non condensing
Overall Size	53mm x 145mm x 160mm (without base) 2.09" x 5.75" x 6.31" inches (without base)
Camera Weight	2.5 lbs/1.14 kg (without base)
Camera Base Options	Magnet Mount, Security Mount, Clicker Base Mount, Permanent Bulkhead Mount, Lightbar Interface Mount, SUV Roof Mount
Safety Feature	Class 1 Illuminator, EN60825-1

MPH M7 Processor Unit



Figure 6: Two Camera M7 Processor

M7 PROCESSOR SPECIFICATONS	
Processing Board	LINUX based RISC processor
Input Power	12 VDC from vehicle battery with 12VDC ignition key signal 2 Camera System: <20W
Interfaces	2 Camera, 1 Power, 2 Ethernet Mil-spec IP67
Housing Protection	IP67
Network Switch	100 Mbit fast Ethernet adapter
Data packet	For each Read system generates; - Read License Plate String - Date-Time Stamp - GPS Coordinates on map - Camera Identifier - JPEG compressed color overview of car - JPEG black/white close-up plate photo
Optical Character Recognition Training	Regionalized OCR optimization
Operating Temperature	-40 – +60'C (-40 – +140'F)
Operating Humidity	10-90%
Processor Dimensions	159 x 298mm x 70mm 6.25" x 11.75" x 2.75" inches
Weight	2.2kg (4.9 lbs.)
Vanity and Special Plates	A special algorithm allows reading non-structured vanity and special plates.

Non-reflective plates	An enhanced power illuminator and special low-contrast algorithms allow system to achieve accurate results where non-reflective plates are in use.
Red ink character plates	IR Illumination unique wavelength allows the system to have accurate results on red ink plates where higher wavelength IR cameras fail to get the necessary contrast.
Software Suite	CD ROM includes 1. Touch screen enabled on-board User Interface with live display of plate reads, alarms management, Hot List management, shift reporting, and data export. 2. Fast bulk-loading hot list software (from USB thumb drive)
Documentation	Software Installation Manual and User Manual

EPHM7 Camera Cables

Cable SPECIFICATIONS	
Connector	8 Pin Military Grade, IP67 rated
Cable	Proprietary 8 Conductor Composite Cable, Jacket-Black Poly Urethane
Dimensions	Connector: 1 inch dia. (30.4mm) (both ends) Cable: 0.35 inch dia (9mm) multiple lengths available

EPHM6 Global Positioning System Antenna

ANTENNAE SPECIFICATIONS	
Interface	USB
Datum	WGS-84
GPS protocol	NMEA or Garmin
Data Rate	4800 bps

EPHM7 CarSystem 6.0 Software Suite



CARSYSTEM SOFTWARE SPECIFICATONS	
Operating System Capability	All released versions of Microsoft Windows 7/8 /10 operating systems.
Connectivity	The system is capable downloading Hot-List data files and uploading ANPR Detection and Hot records via the following methods: • 802.11 Wi-Fi • Cellular
Buffering	All records are buffered if connectivity to the server is interrupted. Once connection is restored, all data transactions that occurred during the interruption are updated in the order of their priority.
Comprehensive Search Utility	Search mechanism enables the operator to search manually: all vehicle detection records, all Hot List records, and/or all Hit activities. Searches can be performed using partial license plate entries
Custom Note Capabilities	The system allows operators to add customized notes to all records and upload them to the server for use by all other operators
System Integrity and Change Tracking	Each record is dealt with as precious information that should never be lost under reasonable operating conditions. The database engine allows for data changes to be made as an atomic operation, which protects against any data corruption as a result of sudden power loss or temporary storage hardware failure. Protection for committed data will also be provided by the database page checksums. Changes are tracked via history tables in the database. This is done for replication to the server database, for auditing purposes, and for record integrity. Changes/audits are searchable on the server and maintain their own retention logic settings.



Data Transmission	The central server has a persistent connection to all in-car systems. Immediately on any change applicable to a particular system, the server transmits updates to Hot Lists and receives all new Reads and Alarm records generated by the in-car system. The communication uses history tables in the in-car system's database to determine what changes must be transmitted between the two systems.
Alarm Notification	While the in-car system is communicating with the server, it transmits all Alarms and Reads to the server. When the server receives an Alarm, and as it processes each Alarm, it checks to see if the Alarm is of a type that requires an email address for notification. If it is, it generates and transmits an email with the Alarm information to that email address. Additionally, whenever an alarm occurs, if the ELSAG Tactical Operations System is running in conjunction with CarSystem, it will send a simultaneous notification to the dispatcher and to other vehicles that are subscribed to that event.
Filtering	Hot lists can be filtered by location (geo-fencing) or by any other search parameter. Hit visibility is determined based on access levels to the particular agency containing that list and the user's current agency
Data Queuing	All data records in queue waiting for transmittal are prioritized by type. A hit's text data, followed shortly by its image data, is always sent before anything else, except confirmations of data received (when in full duplex operation). Additionally, large objects like images, are sent in chunks so that they can be interrupted immediately in case of very high priority data such as hits to be sent. Interrupted transfers will continue where they were left off once network connectivity returns and/or the critical priority data has completed transmission.
Log-In Credentials/Authentication/Privileges	The system allows any number of operators to log into the in-vehicle system. The system administrator controls login credentials. The administrator can set a user's privileges in such a way that they may or may not customize the default settings of certain in-car system features. The system provides each user a unique account. Each account has a user-modifiable profile associated with it. The profile allows the operator to choose the default settings for things like type of alarms that will sound, display language, volume settings, etc. After completing operator authentication, the in-car system will communicate with the central server and synchronize the Hot Lists on the car so that the in-car database contains data only for those Hot Lists that the operator has access to.

Collection and Retention of ANPR Data	The system currently captures the following information when a number plate is read: • The date/time the image was taken; • The date/time the read was recorded in the database; • The ID of the user who was operating the vehicle; • The ID of the organization that owns the record; • The number plate as read by the camera; • The state of the number plate, as determined by the camera; • The country of the number plate, as determined by the camera; • The camera's confidence in the read, on a scale of 1 to 100; • The ID of any Alarm group that was generated from this read; • The latitude of the car's position at the time the read was generated; • The longitude of the car's position at the time the read was generated; • The error radius associated with the car's position; • The car's east to west speed; • The car's north to south speed; • The ID of the group associated with the data owner Each number plate read occupies up to 140 bytes, plus the images. A color overview image occupies about 40K bytes on average while a black and white plate image occupies about 12K on average. That gives a total of about 53K bytes on average per read. The individual read records are maintained in the in-car system's database for a period of time that is set by the system administrator. The retention period can be set to any length desired. Removal of data from the server takes place in the order of oldest records first.
Connection Between CarSystem and Servers	The in-car software periodically connects to the central server automatically and checks for updates to Hot Lists. The update frequency can be configured by the system administrator. The in-car system connection to the server is constantly being monitored and displayed to the user. It also allows the operator to send test messages to the server at any time to ensure proper communication.
Alarm Stacking	After receiving a read from one or more cameras, the in-car system checks for Hot List matches automatically, no matter what the operator is doing with the front-end software. Each match raises an Alarm; all alarms are "stacked" until the operator acknowledges them or they time-out.

Camera Displays	The in-car system can display up to four (4) camera views on the same screen at once. Each view can be toggled between color and IR images and will display a live stream of the reads and data coming from that particular camera.
Alarm/Hit Screen Display	The system Alarm or 'Hit' Screen includes: • Hot-List alert name or type • The Hot-List source name (i.e. US-NCIC, CA-DOJ, etc.) • Includes date the Hot-List record was created or made active • Two images – color overview of vehicle & infrared of the number plate • Each image shall allow user to view in full screen via double click • OCR interpretation of plate • GPS coordinates for location • Narrative comment text, Hot-List notes available • Registered Owner • Vehicle parameters (i.e. make, model, color, etc.) • Camera designated name that scanned matching vehicle • Detection rating to allow the User to: • Designate if read is correct/incorrect • Correct plate read if incorrect
GUI Operation Indicators	The system GUI provides the following operational status indicators to alert the operator when an error or failure has occurred within the system. • Wireless connectivity status between system and ANPR server is either connected or not connected with reason code • GPS satellite signal status indicating if properly receiving with live coordinate display or if not receiving signal with reason code • ANPR camera status of both color and infrared cameras indications if system is receiving video or not receiving video with reason code • ANPR processor status indicating if ANPR processor is properly functioning or if not functioning with reason code

Manual Hot-List Entry	Assuming the administrator has given the necessary permissions, an operator can enter a Hot List record that includes: • Number plate number • State of registration • Alert Name w/ priority status • Up to three custom note fields with titles • Up to 255 character vehicle comment with subject • Set an expiration time period for the Hot-List record to remain active. Subsequent to the expiration date, the Hot-List record shall automatically be rendered as inactive • Distribution to all ANPR systems, server, recorded in the database (and made available to Users with appropriate permissions) and then automatically redistributed through the ANPR network to allow all ANPR systems to receive the Hot-List record as an active target vehicle in which to alert upon. • Notify (via an alert) the user who entered the record prior to the expiration date.
System Response Time	The system compares a captured plate against multiple large databases comprising of more than 3,000,000 records with a less than 2-second response time.
GUI Light Setting Modes	The system GUI is available in both a daytime and nighttime modes that is selectable by the operator if permission is granted by the system Administrator. Nighttime viewing mode decreases the light emitted from the screen during dark nighttime conditions.

View of Camera

Camera Size:

- Standard 12mm (covers 12 feet wide by 15 feet long or 3.6 meters by 4.5 meters) and 16mm (covers 12 feet wide by 24 feet long or 3.6 meters by 7.3 meters). Only one camera on the right is required to perform all plate reading missions including adjacent lanes or parked vehicles (90⁰ or diagonal or parallel parked).

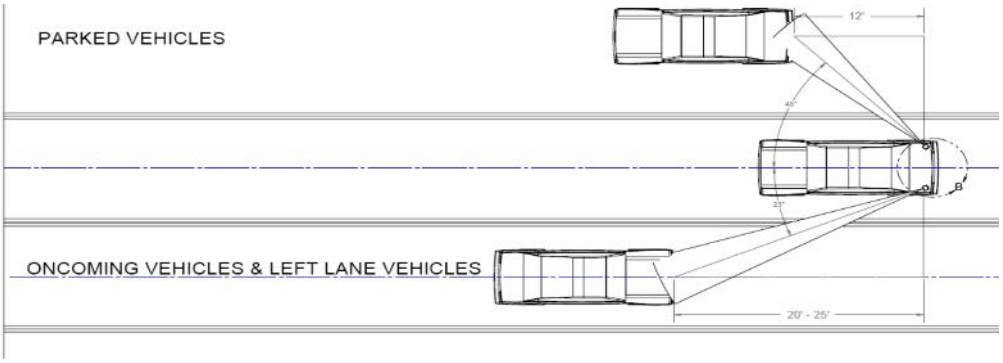


Figure 7 – Camera Range

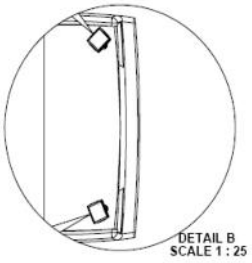
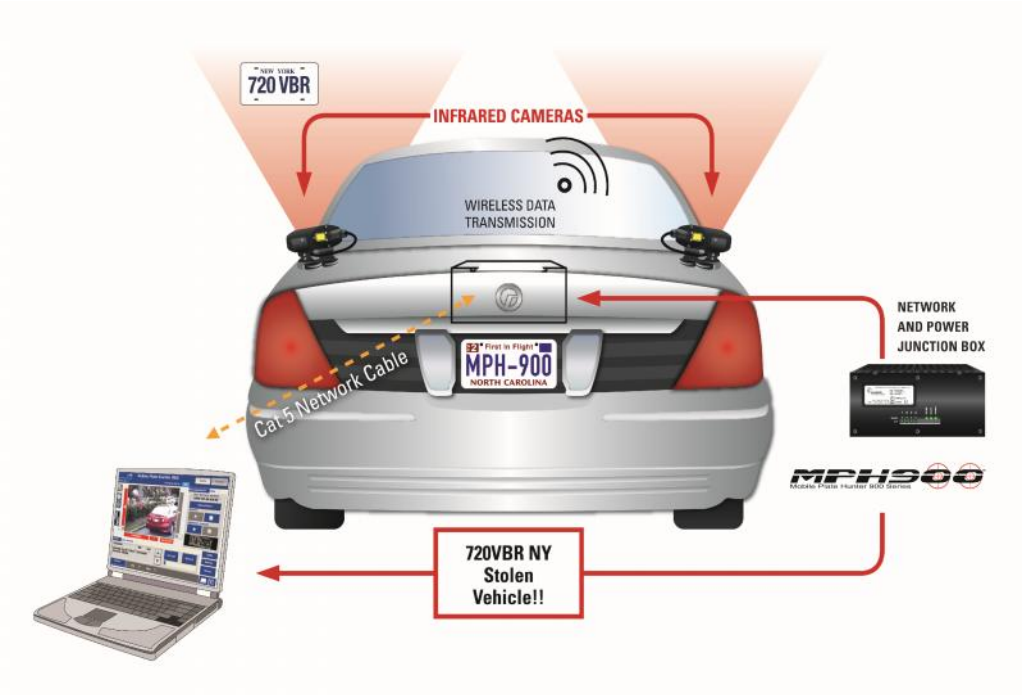


Figure 8- A two camera configuration with trunk mount



Figure 9 – Camera Snapshot comparable to competition.

How It Works



- Infrared cameras read plates of parked and moving vehicles across 4 lanes of traffic.
- Processor Box compares data with Hot List records of suspect vehicles
- Wireless connectivity sends images to software uploaded on Mobile Data Terminal (MDT).
- Alarm sounds when suspect vehicle is passed.



MDT Mobile Data Terminal

Compatibility with on-board PC or Mobile Data Terminals

The ANPR cameras need an on-board PC to host the user interface.
It is usually possible to utilize existing Mobile Data Terminals (MDT) if they comply with the following minimal requirements
The computer on which you install Car System must meet the following requirements at a minimum:

- Intel® Core™2 Duo CPU with at least 2 GB RAM
- 800X600 minimal display Resolution
- 5 GB hard disk space available (more HD space is required for longer retention locally on the PC)
- LAN data port for connecting the PC to the Processing Unit (the Unit must have STATIC IP addresses); if an on-board LAN is already present, a switch port must be available and the IP address of the unit can be adapted for the existing IP class. If a firewall is present, UDP and TCP traffic shall be enabled between the PC and the Unit.
- 1 open USB 2.0 port
- Windows 7 or higher

- The Hot List is a standard TXT file and must be generated by the User. The hot list file is the database of the wanted plates and shall be downloaded onto the on-board PC by means of a USB memory stick. It is also possible to download the Hot List wirelessly by means of Wi-Fi or cellular broadband.
- The on-board MDT may be optionally touch screen enabled
- GPS devices, compliant with NMEA 0183 version 2.0 or later, can be installed on any serial (COM) or USB port; if available all the read license plate could be associated to a location for further analysis.

Operations Center Software Suite – Enterprise Operations Center (EOC)

(to be ordered as a separate item)

When a fleet of cars are equipped with MPH™900 or if it is preferable to have a separate workstation placed in an office environment for after action analysis, the optional Operation Center software is the right solution. Wireless communication capability allows automatic Hot List download and mission data upload. An ANPR unit that maintains a wireless connection to the EOC will receive an automatic data download to include the most up to date hot list.

The EOC provides archiving of all the collected data (both alarms and normal reads) as well as database search functions. An included mapping module allows the system to display alarms and reads on a map.

Cellular high-speed networks are supported.

Wireless network deployment and installation is not included. The design of the wireless network can be provided as a separate service.

Not included:

OP-Center Server PC with the following minimal requirements.
This Server configuration example below is for less than 5 mobile units and data storage for up to 6 months.
If the requirements exceed these constraints the Server specification must be evaluated on a case by case basis and a hardware sizing guide is available.

SERVER	
Functions	Aggregator, Trans DB, Staging DB, Web Service, Image Storage
Minimum	Intel i7 Quad Core
Recommended	Intel Xeon Dual Core
RAM	
Minimum	16 GB
Recommended	32 GB
Hard Drive	
OS	7.5k RPM, 100GB (page.sys located here)
IMAGES	7.5k RPM, 100GB to 750GB/yr *See Capacity Planning Worksheet
SQL	7.5k RPM, *See Capacity Planning Worksheet (meta data storage - no images)
Software	
OS	
Minimum	Windows Server 2008 R2 64bit version, Windows 7 Professional 64bit
Recommended	Windows Server 2012 R2 64bit version
SQL	Microsoft SQL Server 2008 R2, or 2012 or 2014 (any version) 64bit versions
.NET	
Minimum	.NET 4.6 required
Recommended	.NET 4.6.2



Custom Hot List Input Format

Adaptation software will be provided to convert any kind of input text file into the proprietary system format.

Maintenance and Support

Warranty Year 1	Included
On Site Training	Included
Phone Support	Included

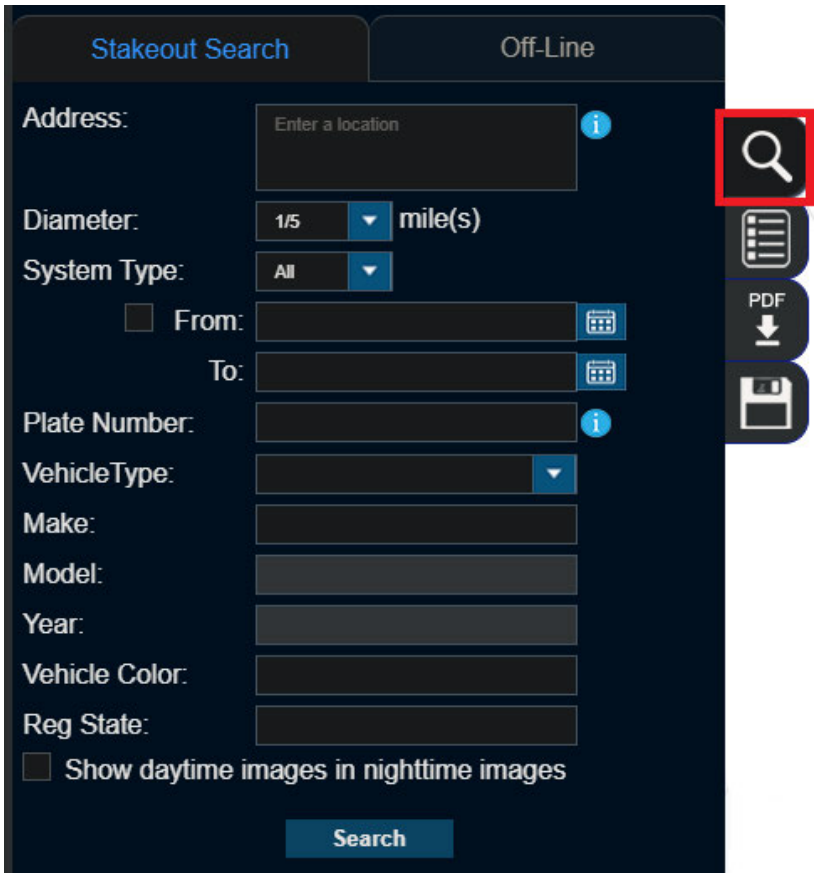
VIGILANT VEHICLEMANAGER QUICK GUIDES

STAKEOUT

This guide describes how Users can use the **Stakeout** feature of VehicleManager to search for vehicle detections grouped by their visits to a location.

- **Stakeout** searches a 4 mile radius defined by address or geozone for vehicles that have visited that location themselves, or along with a specific target vehicle in a specified time frame. Locations must have detections made by a CarDetector system from within the geozoned boundary to return results. Only an address is required to perform a Stakeout search, but additional details will help narrow the results and make them more useful.
- The **Visits Tab** filters results to include only visits made along with the target location vehicle, or only visits made by the target vehicle.

PERFORMING STAKEOUT SEARCHES



1. Login to VehicleManager and navigate to **Stakeout**.
2. To perform a Stakeout Search, click on the **Search Tab (Magnifying Glass)** and then the **Stakeout Search** tab.

© 2023, Motorola Solutions. All rights reserved. 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.

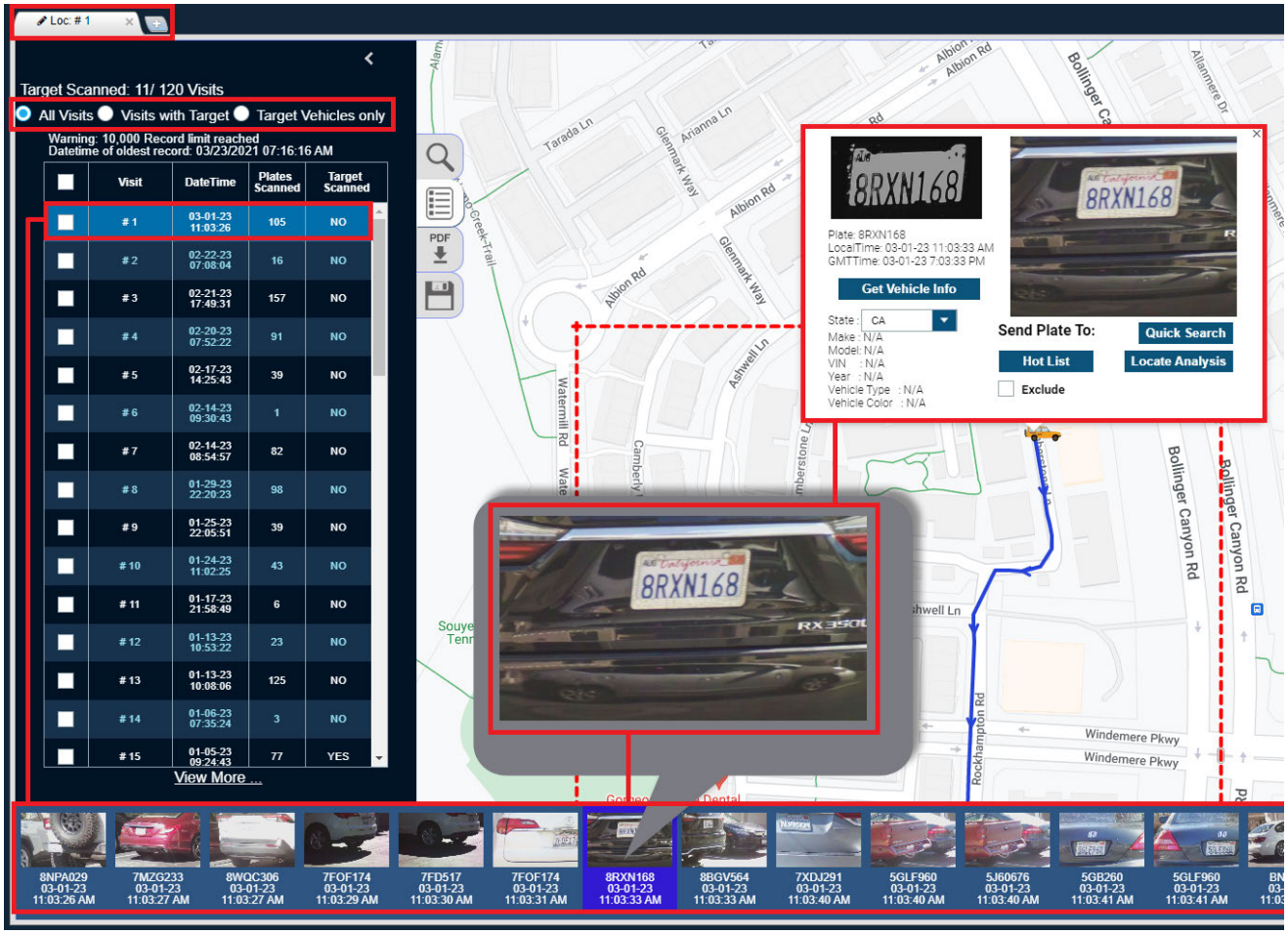
3. Select from the following options to define a search address and a target vehicle:

	Option	Description
1	Geo-zoned Locations	Select from a list of pre-made Locations defined by a geozoned border. Locations are created and managed by Site Managers.
2	Address	Enter an address to focus the map on that location.
3	Radius	Instead of using a geozone, use this value as the largest distance from the address that will be searched. The radius is limited to 2 miles to prevent long search times. **NOTE:** This option is disabled when a Geo-zoned Location is selected.
4	System Type	Search for detections made by fixed systems, mobile systems, or both.
5	From/To Date	Enable the checkbox and click on the **Calendar Icons** to set a date and time range. Only detections made within this period will be returned in the search results.
6	Plate Number	Enter a single license plate number to search for. Click on the **Information (i)** icon to view formatting rules for performing wildcard searches.
7	Minimum Speed	Set a minimum speed for vehicle detections by systems with speed calibration enabled. Only detections generated by vehicles traveling at a speed greater than this value will be returned.
8	VehicleType	Set a type of vehicle to be searched for.
9	Make	Click to view a list of vehicle makes and set a specific vehicle Make to be searched for.
10	Model	If the vehicle make is set, click to view a list of that vehicle make's models and select a specific model to search for.
11	Year	If the vehicle make is set, click to set the make or model year to search for.
12	Show daytime images in nighttime images	If the search returns detections that were made at night, this option enables the overlay of a detection from the same vehicle made during the day on to the nighttime image. This is useful for verifying visual details about the vehicle.

4. Click **Search** to perform the search. Results will be displayed in the **Visits** tab and on the map.

© 2023, Motorola Solutions. All rights reserved. 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.

VIEWING RESULTS IN THE VISITS TAB



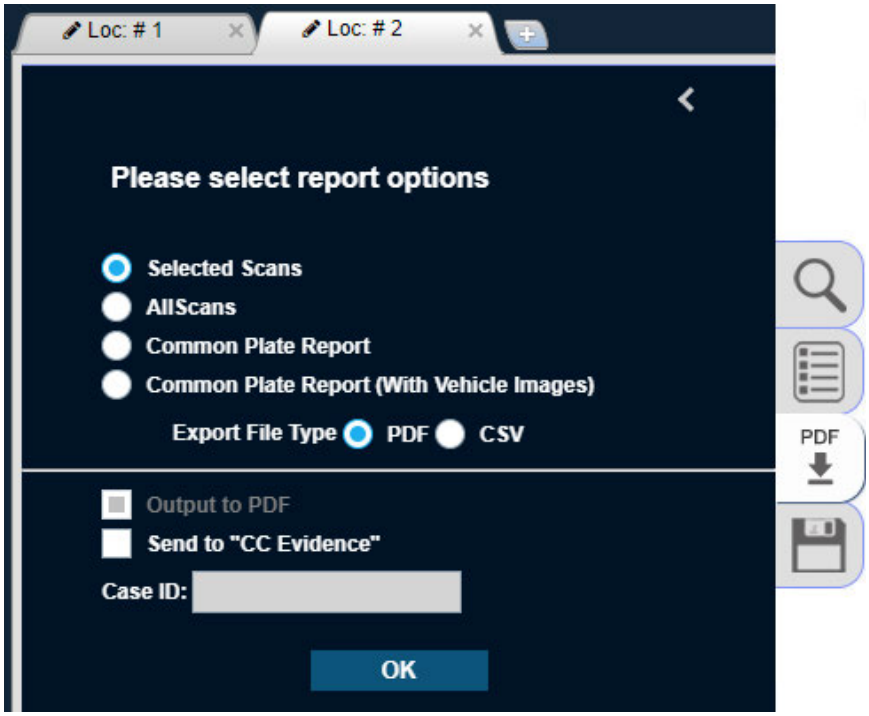
1. In the **Visits** tab, select from the filtering and tabbing options to view the search results:

Option	Description
Visits List	A selectable list of all the detections made in the location, grouped by visit.
Detection Filmstrip	A selectable list of each detection and plate image made during the visit.
Location Tabs	Use the **Plus (+)** sign at the top of the map to create a new location tab. Up to 30 location tabs can be created. Each search will be shown on the map by a pin with a corresponding tab number. Right click on a tab to **Rename**, **Duplicate**, or **Close** it.
All Visits	View all visits made by vehicles to the location.
Visits with Target	View only vehicles that visited the location with the target vehicle searched for in the search tab.
Target Vehicles Only	View only visits made by the target vehicle searched for in the search tab.

© 2023, Motorola Solutions. All rights reserved. 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.

2. Click on a visit in the **Visits List** to populate the **Detection Filmstrip**. Hover the mouse over a detection to view an enlarged plate image. Click on the detection to show the vehicle information popup.

GENERATING STAKEOUT REPORTS



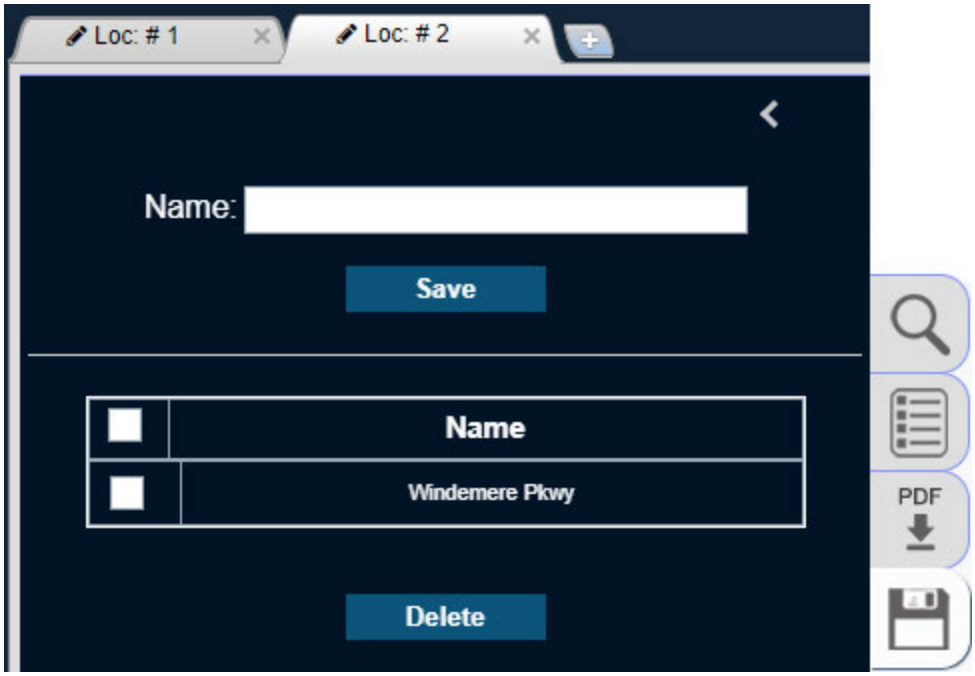
The **Report Tab (PDF)** generates reports from the search results. To generate a **Common Plate Report**, two location tabs must be open and have active searches in them. Large reports may be generated without images to speed up the process.

1. To generate a report of the search results, click on the **Report Tab (PDF)**.
2. Select from the reporting options:

Option	Description
Selected Scans	Only the checkmarked scans in the visits tabs of each location will be included in the report. Each location is sent as a separate report combined in a .zip file.
All Scans	All scans present in the visits tabs of each location will be included in the report. Each location is sent as a separate report combined in a .zip file.
Common Plate Report	Each location and any detections common to both locations will be included in the report.
Export File Type	Choose a file format to receive the report as: **.PDF** or a **.CSV** file

© 2023, Motorola Solutions. All rights reserved. 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.

SAVING STAKEOUT SEARCHES

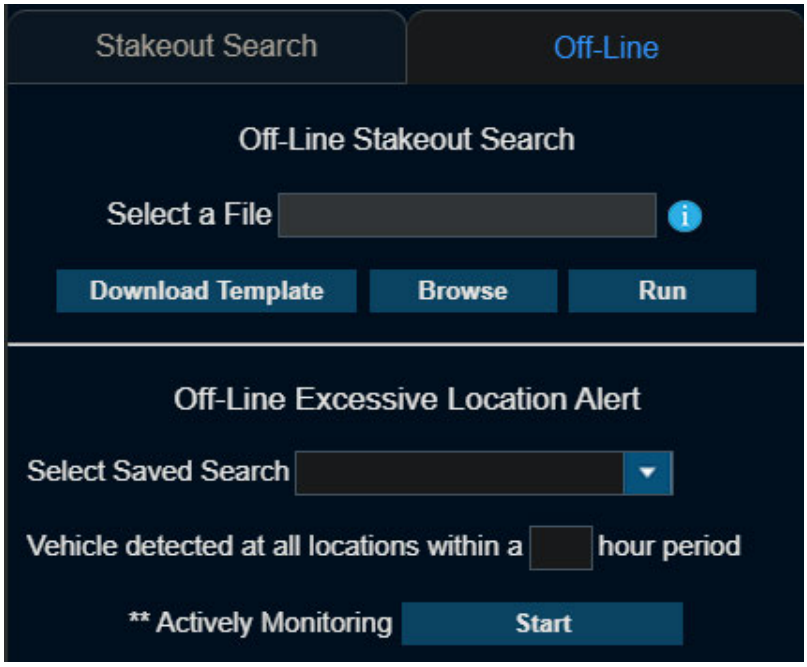


The **Save Tab (Disk Icon)** saves the search results from the currently selected location tab. Saved searches can be re-opened later in a new location tab.

1. To save the current search, click on the **Save Tab (Disk Icon)**.
2. Enter a name for the saved search and click **Save**.
3. To open a saved search, use the **Plus Sign (+)** to open a new location tab and click the **Save Tab (Disk Icon)**. Click on a saved search to re-open it.
4. To delete saved searches, check the boxes next to each search to be deleted and click **Delete**.

© 2023, Motorola Solutions. All rights reserved. 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.

PERFORMING OFF-LINE STAKEOUT SEARCHES



Off-Line Stakeout Search functions like Stakeout Search but without the search radius limitations. Offline searches take longer, but are processed by the server in the background and delivered to the specified emails when compilation is complete. Offline search parameters are defined in a .XLS file and uploaded to VehicleManager. Use Off-Line Stakeout Search when the area to search is large or there are many locations to search.

1. To perform an Off-Line Stakeout Search, click on the **Search Tab (Magnifying Glass)** and then the **Off-Line** tab.
2. Click the **Download Template** button to download a .XLS file with pre-filled headers. For each row, define a Unique Location Name, Address, and search radius in miles.
3. Select a period in hours or days to search into the past, during which detections must have been made to be returned in the search results.
4. Click **Browse** and select the completed template file with the search locations and radii.
5. Click **Run** to begin the search operation. The results will be sent as a .PDF or .TXT file to the User's email address on file.

© 2023, Motorola Solutions. All rights reserved. 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.

OFF-LINE EXCESSIVE LOCATION ALERT

Off-Line Excessive Location Alert uses a saved Stakeout Search to monitor the locations defined by the search off-line and will deliver email alerts to the specified email address when a target vehicle is detected at any of the locations within a set period of hours or days.

This feature is useful for investigating vehicles that consistently visit multiple locations within a set time period.

1. To begin off-line excessive location alerting, configure the desired search areas and target vehicles in the **Stakeout Search** tab. Use the **Save Tab (Disk Icon)** to save the search.
2. Return to the **Off-Line** tab and select the saved search in the **Select Saved Search** dropdown menu.
3. Enter an email address in the **Email addresses** field to send the alerts to. To send alerts to more than one email address at once, separate each address with a semicolon (;).
4. To send alerts when a vehicle visits each of the search locations within a certain period of time, set the period in hours or days in the **Vehicle detected at all locations** field and drop down menu.
5. Click **Start** to begin the monitoring.

© 2023, Motorola Solutions. All rights reserved. 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.

SUPPORT

For assistance with the topics covered in this guide or with any Vigilant product, please contact the Vigilant Training Team or any of the Client Relations Managers below. **Please send us your software update ideas and success stories!**

CHRIS SCANDOLE
Manager, Client Relations, PS
Central Region – US
(917) 913-3351
christopher.scandole@motorolasolutions.com

LEE YONEMURA
Manager, Client Relations, PS
West Coast – US
(916) 307-0893
lee.yonemura@motorolasolutions.com

DAVID RIVERA
Manager, Client Relations, PS
Southeast Region – US
(813) 460-6993
david.rivera1@motorolasolutions.com

CHRIS PITTMAN
Manager, Client Relations, PS
South Central – US
(469) 712-3060
chris.pittman@motorolasolutions.com

SAM PALMER
Manager, Client Relations, PS
North Central – US
(480) 549-2901
sam.palmer@motorolasolutions.com

MARCIA BRODERICK
Director, Client Relations Nationwide
(279) 201-4142
marcia.broderick@motorolasolutions.com

MIKE PRATE
Manager, Client Relations, PS
Northeast Region – US
(934) 500-9658
michael.prate@motorolasolutions.com

VIGILANT TRAINING TEAM
VigilantTraining@motorolasolutions.com

© 2023, Motorola Solutions. All rights reserved. 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.

TRAINING

For free training, visit VSLEA.ORG



THANK YOU, AND STAY SAFE!

© 2023, Motorola Solutions. All rights reserved. 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.

Massachusetts Department of State Police
Automated License Plate Recognition (ALPR) System
Memorandum of Understanding and Agreement

THIS AGREEMENT, made and entered into this **Twenty-Third** day of **March, 2023** by and between the Department of State Police, hereinafter referred to as "Department," and the **City of Taunton – 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.

Colonel John E. Mawn, Jr.
Massachusetts State Police

Representative: **Edward J. Walsh, Chief**
Agency: **Taunton Police Department**

Date

03/28/2023
Date



Maximizing installation performance

Part 3 – Time Settings

Neology UK

28th April 2021

Time Settings

Q: Why do we care about the time?
A: All events are stamped with a time. Without an accurate clock, the event may become “unusable” because we can no longer be sure the time is correct.

Q: Why do we need an external time-source?
A: The camera cannot know the correct time on it’s own – it needs an “authoritative” time source to tell it the correct time. This can be either an external NTP server (which will have further time-sources of it’s own), or a GPS receiver to use the GPS satellites as the time-source.

Q: How do we check if the time is good?
A: The camera tracks whether time is synchronized with an external time source and reports this status in the logs. It can also stamp images with this status.

Q: Are all “time not synchronized” events useless? Shouldn’t we just delete all events without time sync?
A: Not necessarily – just because time is not synchronized it does not necessarily mean the clock is wrong – just that we can no longer be 100% sure it is correct. Assuming time was previously set correctly, it is expected that time will only drift by small amounts, so long as synchronization is not lost for a long time. The sequence of events is also still likely to be correct, and so there may be independent ways to verify the times.

Copyright © 2021 Neology, All Rights Reserved.

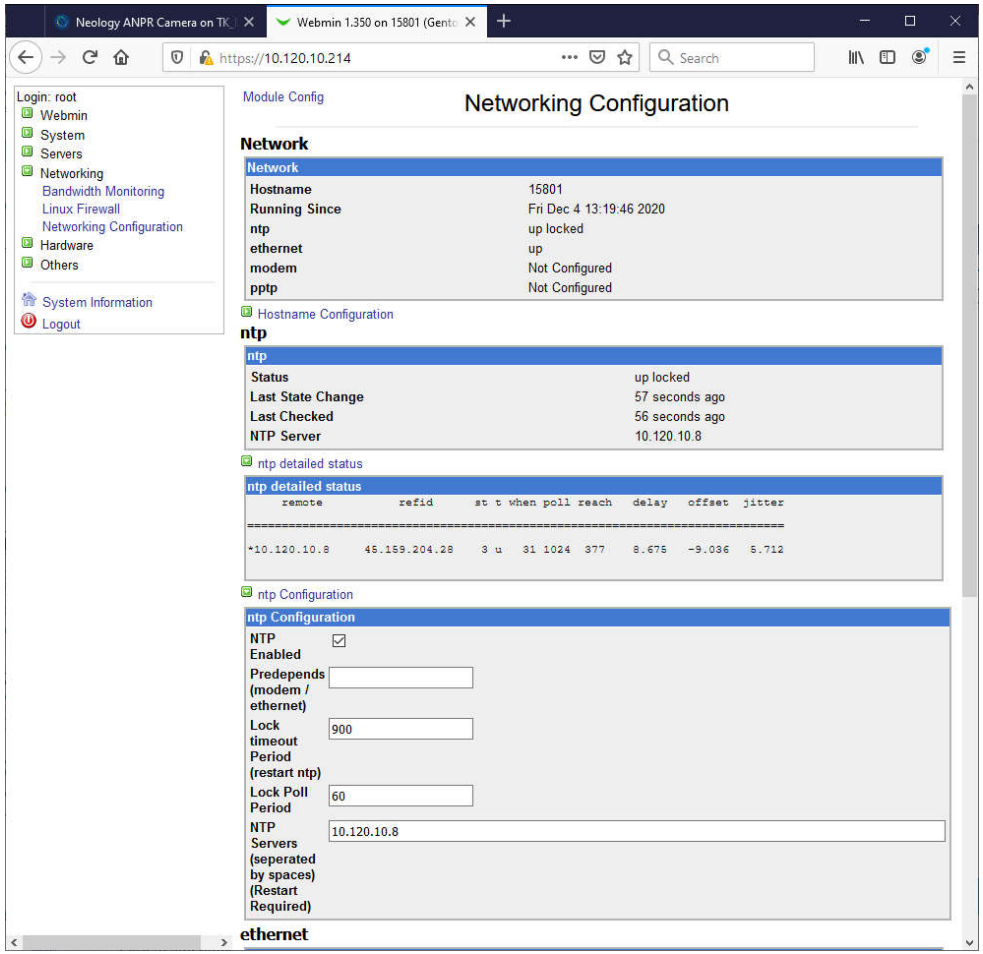
Time Settings – Key Concepts

Concept	Purpose
Camera system time	Tracks the current time according to the camera, and is the clock used when stamping events with timestamps.
Camera hardware clock	Battery backed “realtime clock” chip in the camera used to set initial camera system time when the camera has been powered down.
“Network Time Protocol” (NTP)	NTP is an industry standard mechanism for synchronising clocks between devices. On start-up it will synchronise the local system time to the same as the remote server, and then tracks that the clocks remain synchronised.
Timezone + UTC offset	System time, hardware clock, and NTP all use “UTC” – the timezone for the camera should be set if local-time output is desired.
GPS as time source (not available on P492)	If your camera has a GPS device this is a reliable time-source, and can be used with NTP to get very accurate times regardless of network comms.

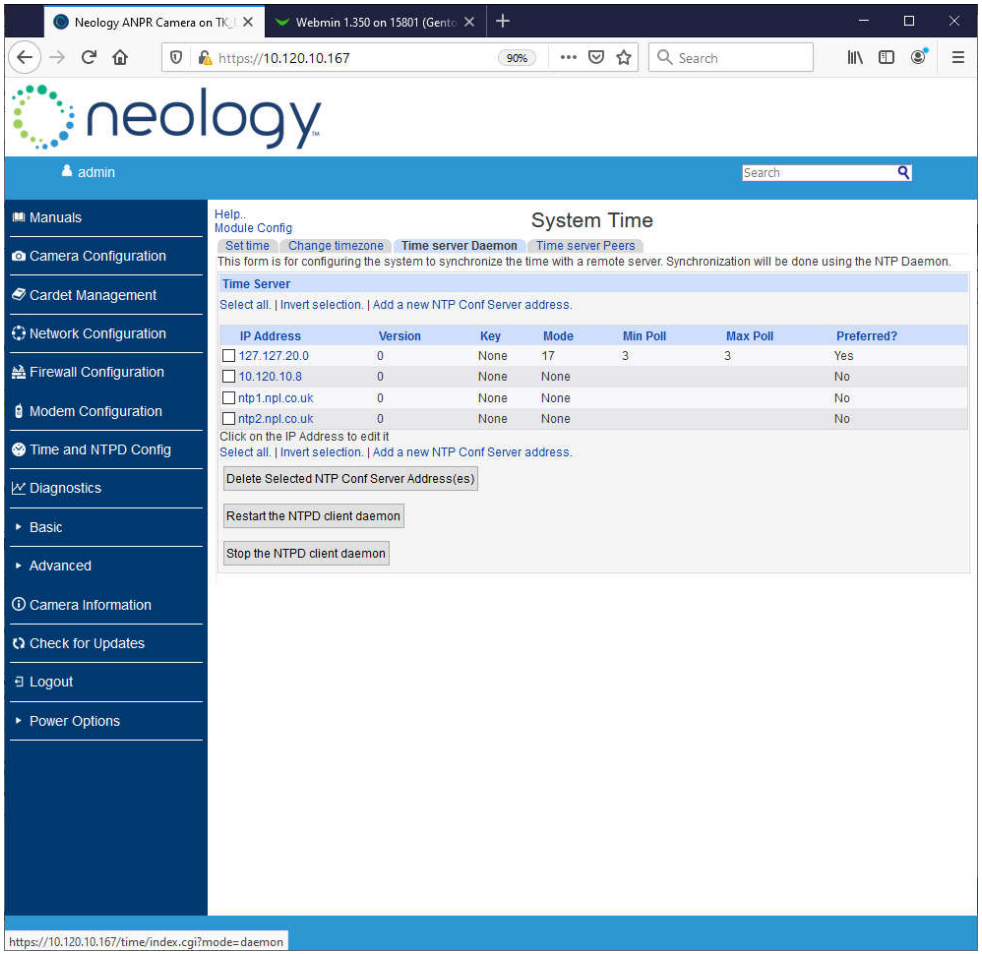
Copyright © 2021 Neology, All Rights Reserved.

Time Settings – Setup examples – NTP

P492



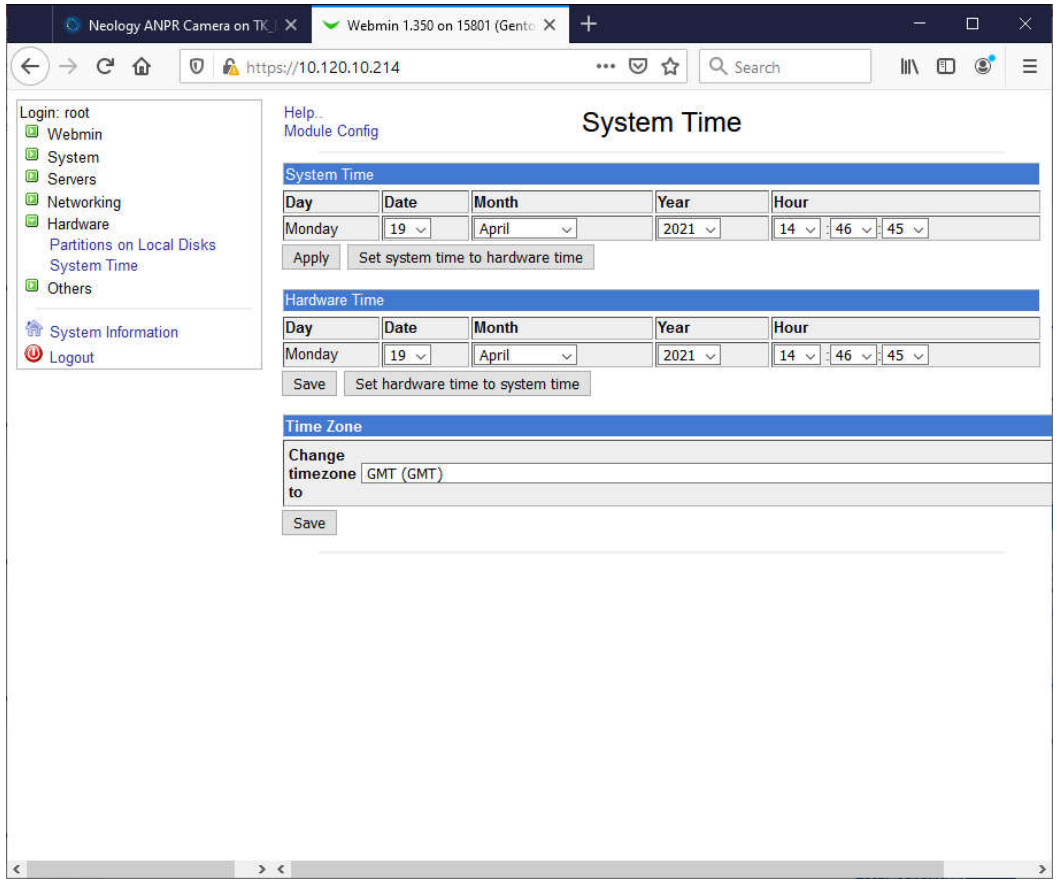
IRIS



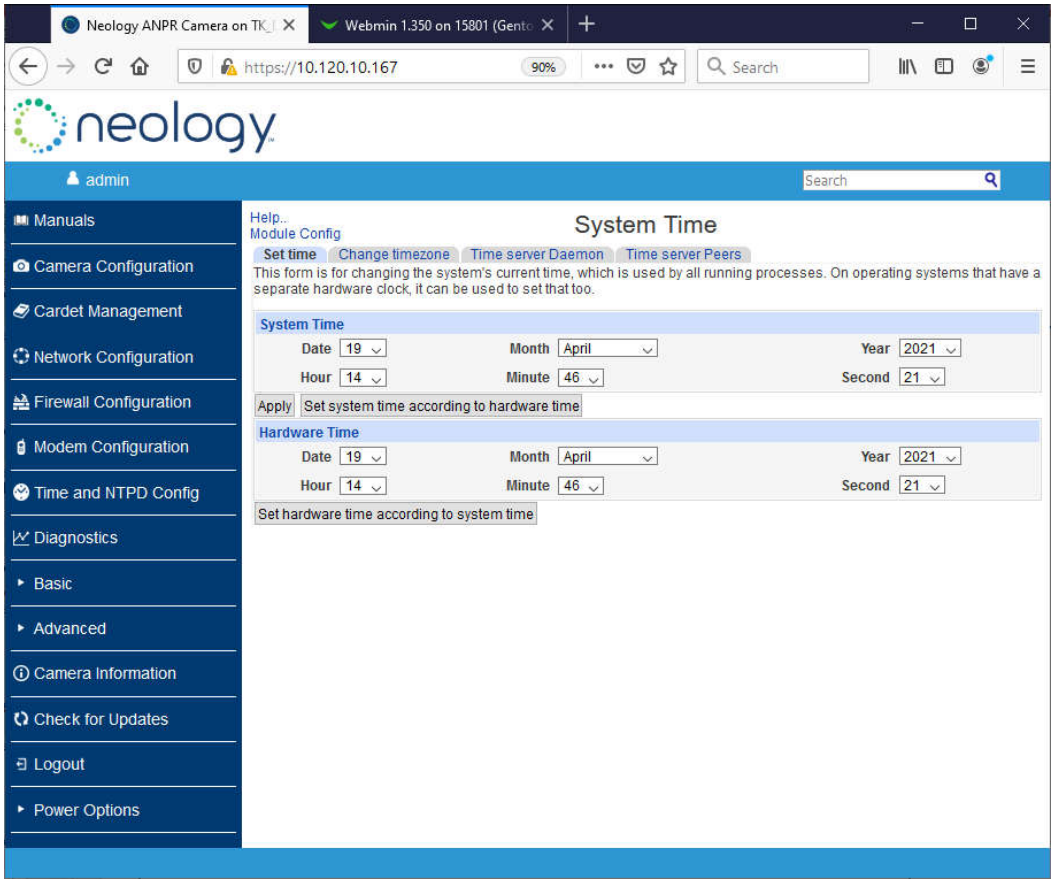
Copyright © 2021 Neology, All Rights Reserved.

Time Settings – Setup examples – System Time

P492



IRIS



Copyright © 2021 Neology, All Rights Reserved.

Time Setting – NTP lock status

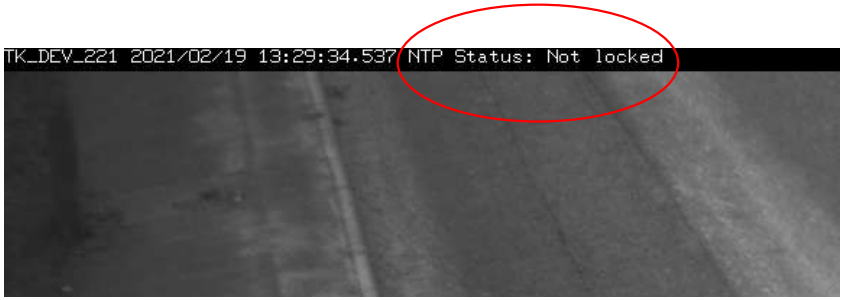
NTP status can be placed in each image alongside the timestamp, and other useful metadata such as “site id”, or GPS coordinates.



Overview Image



NTP Locked

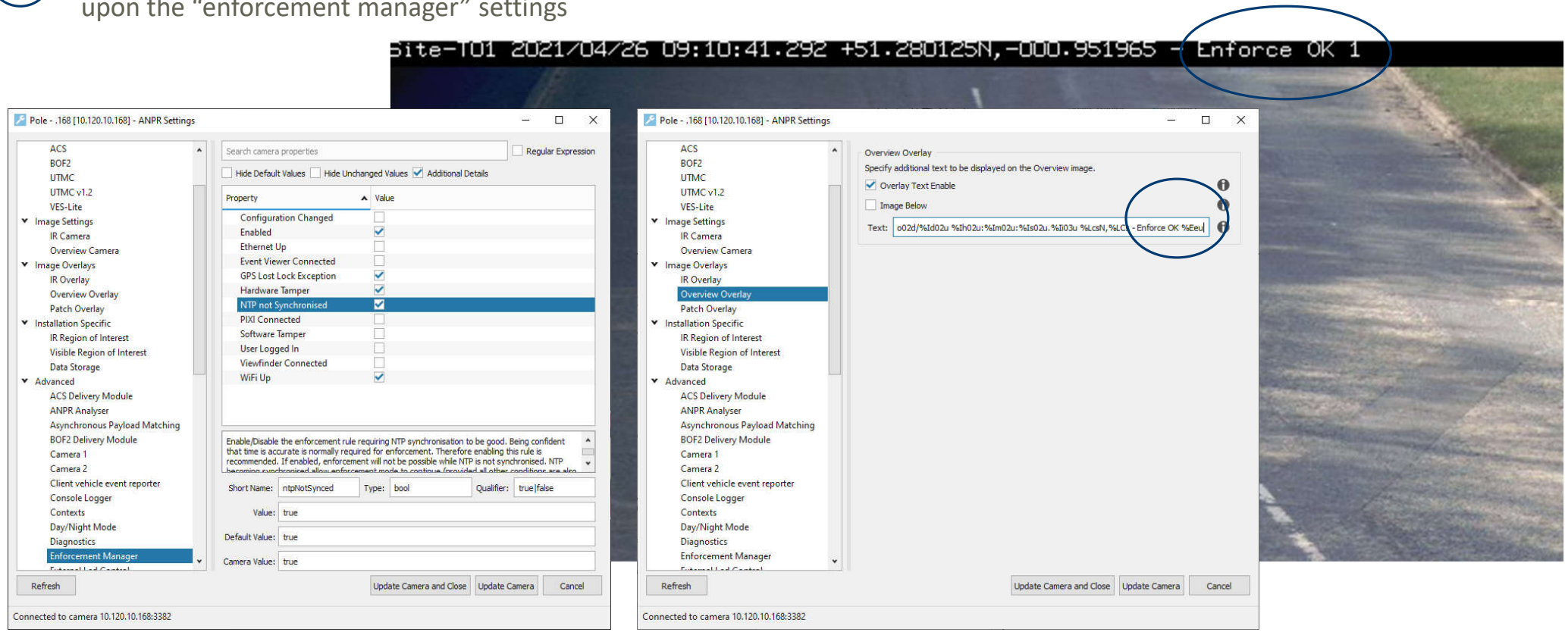


NTP not available

Copyright © 2021 Neology, All Rights Reserved.

Time Setting – Enforcement mode

In addition to reporting the NTP status in the overlay, the IRIS camera can also report the “ok to enforce” status based upon the “enforcement manager” settings



Copyright © 2021 Neology, All Rights Reserved.

NTP and Time Deep Dive

Copyright © 2021 Neology, All Rights Reserved.

Deep Dive – NTP - Overview

- NTP is an industry standard mechanism for synchronising clocks between devices. On start-up it will synchronise the local system time is the same as the remote server, and then tracks that the clocks remain synchronised.
- NTP is used in almost all internet connected devices – Windows and Linux PCs, phones, web-servers, “Internet of Things” devices etc.
- In almost all cases, it shouldn’t be necessary to worry about details of exactly how it works, beyond simply knowing the answers to two questions:
  - Is NTP enabled and configured with a remote peer?
  - Is NTP currently synchronized?
- The answers to those two were covered earlier, but for those who want to know more detail of what exactly NTP does, this “deep dive” can answer some further questions.

Copyright © 2021 Neology, All Rights Reserved.

Deep Dive – NTP – Process

- Fundamentally, the process for NTP is that:
  - On start-up, request the current time from an external time-source (“peer”). If the time is different to the current system time, update the system time to match the peer.
  - After start-up, constantly keep track of the time on the remote peer, monitoring the offset and jitter between the local system time and the remote time, while measuring and taking account of time taken to communicate with the remote peer.
  - During this time, parameters for the local clock are tuned to “speed up” or “slow down” the clock if it is observed the clocks are drifting apart, such that the two clocks will remain in sync with each other.
  - If access to the external time-source is lost, such that the local system time cannot be verified as in sync, then the time will be marked as “not locked”, although that does not necessarily mean the time is wrong. Indeed, the time should remain accurate for many hours.

Copyright © 2021 Neology, All Rights Reserved.

Deep Dive – NTP – Process

- On top of standard Linux functionality, Neology cameras additionally:
  - Monitor if the NTPD process has stopped and will automatically restart it if it isn't running.
  - Monitor if the remote peer is marking as "not synchronized" and record this fact in it's logs and event metadata.
  - Make configurable the number of polls missed before reporting the time as "not locked" to warn of comms failures with NTP earlier. (NTP only flags a loss of synchronization after 8 missed polls).
  - On IRIS the optional GPS receiver may be used:
    - As a "stratum 0" time source for NTP.
    - To discipline a second clock independent of NTP and the system clock. This provides an independent clock that can used to verify the NTP controlled system time.

Copyright © 2021 Neology, All Rights Reserved.

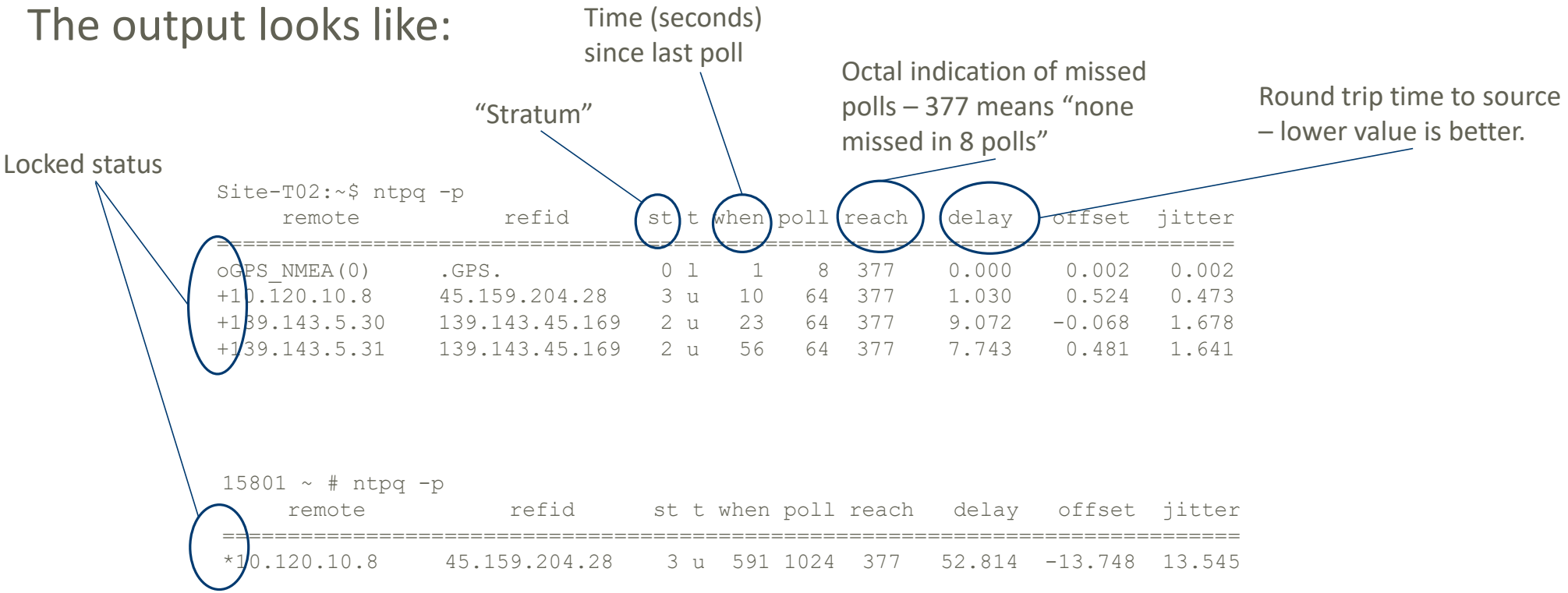
Deep Dive – NTP – Polling frequency

- Default behavior of ntpd:
  - On startup it will poll once every 64 seconds
  - It will gradually increase the period between polls, 64s, then 128s then 256s eventually settling on once every 1024 seconds (1024s = approximately 17 minutes).
  - The ntpd itself will only flag “loss of synchronization” after 8 consecutive polls have been missed (no response). The expectation is that the time will remain stable for at least that long.
  - Assuming ntpd has reached its final poll period of 1024 seconds, it will take **2 hours 16 minutes and 32 seconds** before ntpd reports a remote peer as lost sync. However to reach this level, the local clock must have been synchronized for a long time already, and so the clock parameters should have been tuned to minimize drift.
- It is possible to adjust the polling frequencies (although it remains non-linear), however it is **strongly recommended** that these parameters are left at the defaults, as adjusting these has an impact on the accuracy of the time.

Copyright © 2021 Neology, All Rights Reserved.

Deep Dive – Understanding NTPQ output

- The camera is monitoring the output of NTP, but this can also be inspected manually via Webmin / command line.
- The output looks like:



Copyright © 2021 Neology, All Rights Reserved.

Deep Dive – Time – Interactions with power failures

- Neology cameras have RTC (“Realtime clock”) chips which should keep the clock “ticking” even in the case of power failures – although obviously not synchronised to a remote server.
- However, these are battery (or in some cases “super-capacitor”) powered, and so can run out of power.
- If the RTC power fails, system time may be reset to some default / unpredictable state, and the camera will not know that this has occurred until time is successfully synchronized again with an NTP remote time source.
- **However**, the camera will know that NTP is not synchronised at this time, so it’s “ok” for the camera to be in this state so long as the NTP status is checked.

Copyright © 2021 Neology, All Rights Reserved.

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**TRF-11**
Subject:	
Automatic License Plate Recognition	

Policy

The availability and use of the Automatic License Plate Recognition (ALPR) System provides opportunities for enhancing the productivity and effectiveness of law enforcement agencies. The ALPR System also provides opportunities to increase public and officer safety.

The 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.

Purpose

To establish guidelines and procedures for the proper use and application of the ALPR System within the Department of State Police, and to provide guidelines and principles for the collection, access, use, dissemination, and retention of ALPR information by members 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.

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 through, utilization of the ALPR System.

ALPR Data Query Logs: A record of a search or query of ALPR data.

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.

Definitions and Acronyms, continued

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, Incapacitated or Endangered Persons, 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.

Authorized Uses

The provisions of this policy are provided to support authorized uses of ALPR information. Authorized uses may include, but are not limited to, the following:

- Investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime;
- Enhance Department's AMBER/SILVER or other law enforcement alerts and real-time response capability by deploying and networking ALPRs across the state to more rapidly identify and locate vehicles related to potential child-abduction or other serious crimes;
- Alert law enforcement that a particular license plate on a "hot list" (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 and assist in locating dangerous and wanted individuals;
- Identify plates associated with potential witnesses and/or victims of crime;
- Support the Department's homeland security mission by protecting critical infrastructure from subjects who intend to damage or disrupt the systems and locations that allow for travel and the free flow of commerce;

Authorized Uses, continued

- Identify vehicles linked to stolen license plates or other motor vehicle traffic violations;
- Provide situational awareness for law enforcement related to public safety or otherwise relevant to their authorized duties;
- Support local, state, federal, and tribal public safety departments in the identification of subjects associated with/as targets of criminal investigations;
- Support law enforcement response to critical incident responses and special events;
- Support special operations, such as high-crime-area patrols, gang investigation/suppression, operating under the influence initiatives, enforcement details, directed criminal investigations, and other investigations; and
- Support emergency and public safety situations including, but not limited to terrorist threats, kidnappings, missing persons, and felons actively traveling to or from a crime scene.

ALPR Administrator

The Division Commander of Field Services (DFS) shall:

- Designate a 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:

- Ensure the proper selection of personnel approved to operate the ALPR System and maintain an adequate number of trained and authorized users;
- Authorize any requests for ALPR System use or data access according to Department policy;
- Coordinate with all Divisions to ensure resources are available and deployed to meet Departmental investigative needs;
- Ensure 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;
- Designate users who have been properly trained in the use and operational protocols of the ALPR System;
- Allow access to the ALPR System for those users with an approved login and password; and
- Ensure that any changes in hardware, software, policy, or law are the subject of continuing in-service training or bulletins.

ALPR Procedures

The use of ALPR technology shall be approved by the Colonel/Superintendent or designee.

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 members of this Department or by other law enforcement agencies through the ALPR Administrator.

ALPR Operations

Members using the ALPR System shall:

- Ensure, at the start of each shift, 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.

ALPR Alerts/Hits

The member shall, prior to initiation of a stop based on an ALPR Hit or Alert:

- Visually verify that the vehicle plate number matches the plate number run by the ALPR System, including both:
  - Alphanumeric characters of the license plate; and
  - The state of issue.
- Verify the current status of the plate through:
  - The Commonwealth's Criminal Justice Information System (CJIS), or
  - National Crime Information Center (NCIC), or
  - Department's Records Management System (RMS), or
  - Another appropriate source of data, as soon as practicable.

ALPR Alerts/Hits, continued

License plate numbers and date/time location collected through an ALPR, when taken alone, may not be sufficient to identify the individual associated with the vehicle. The Department may be able to link the ALPR information to an individual through, or in combination with, additional information from other sources, such as a check of vehicle registration. It is thus the investigative process that ultimately identifies individuals and not solely a reliance on the information obtained from the ALPR system's automated collection of license plate numbers.

Manual Entry of Data/Manual Hot List

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);
- Investigative needs;
- 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 one (1) year or less.

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.

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;

ALPR Data: Logs, Sharing, Dissemination, and Retention, continued

- 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 and/or intimidating any individual or group;
- Targeting of any individual or group by means of camera placement or data use in a discriminatory manner; and
- Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

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 (i.e., the identity of an individual could be directly or indirectly inferred by using information that is linked or linkable to that individual).

Information 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 point of contact, in writing or electronically, when the Department's ALPR information is alleged, suspected, or found to be erroneous or deficient.

Security

The following shall apply to ALPR system and information security:

- The Department of Criminal Justice Information Services of the Executive Office of Public Safety and Security will operate ALPR servers in a secure facility protected from external intrusion and will utilize secure internal and external safeguards against network intrusions. Any access to DCJIS ALPR information from outside the facility will be allowed only over secure networks;
- The Department and DCJIS will store ALPR information in a manner that ensures that it cannot be added to, modified, accessed, or purged except by personnel authorized to take such actions;
- Access to Department ALPR information will be granted only to personnel whose positions and job duties require such access and who have successfully completed a background check and training;
- Usernames and passwords to ALPR information are not transferrable, must not be shared by Department personnel, and must be kept confidential;
- Queries made to the Department's ALPR information will be logged into the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit; and
- The Department and DCJIS will maintain an audit trail of accessed, requested, or disseminated Department-held ALPR information. The audit trail will be retained for a minimum of one year. It will include all requests for access to ALPR information, the specific purposes for each request, and what ALPR information was disseminated to each individual in response to that request.

State Central Repository

The Department has agreed to:

- Electronically submit captured ALPR data to the state repository maintained by the DCJIS at the Commonwealth's Public Safety Data Center.

The Department and its users agree to the terms of this policy and to the Commonwealth of Massachusetts *Global Justice and Public Safety Information Sharing Policy* of the DCJIS.

Policy Review

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.

Because existing technology may progress and new technology may develop, giving rise to both legal and technological issues, the Department will monitor and assess the appropriateness of this policy, and make amendments as necessary.

References: Executive Office of Public Safety and Security (EOPSS) – The Commonwealth of Massachusetts Global Justice and Public Safety Information Sharing Policy;
EOPSS – Department of Criminal Justice Information Services – Automatic License Plate Recognition System Central Repository Companion Policy;
MPAC: 41.3.9.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**TRF-11**
Subject:	
Automatic License Plate Recognition	

Policy

The availability and use of the Automatic License Plate Recognition (ALPR) System provides opportunities for enhancing the productivity and effectiveness of law enforcement agencies. The ALPR System also provides opportunities to increase public and officer safety.

The 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.

Purpose

To establish guidelines and procedures for the proper use and application of the ALPR System within the Department of State Police, and to provide guidelines and principles for the collection, access, use, dissemination, and retention of ALPR information by members 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.

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 through, utilization of the ALPR System.

ALPR Data Query Logs: A record of a search or query of ALPR data.

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.

Definitions and Acronyms, continued

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, Incapacitated or Endangered Persons, 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.

Authorized Uses

The provisions of this policy are provided to support authorized uses of ALPR information. Authorized uses may include, but are not limited to, the following:

- Investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime;
- Enhance Department's AMBER/SILVER or other law enforcement alerts and real-time response capability by deploying and networking ALPRs across the state to more rapidly identify and locate vehicles related to potential child-abduction or other serious crimes;
- Alert law enforcement that a particular license plate on a "hot list" (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 and assist in locating dangerous and wanted individuals;
- Identify plates associated with potential witnesses and/or victims of crime;
- Support the Department's homeland security mission by protecting critical infrastructure from subjects who intend to damage or disrupt the systems and locations that allow for travel and the free flow of commerce;

Authorized Uses, continued

- Identify vehicles linked to stolen license plates or other motor vehicle traffic violations;
- Provide situational awareness for law enforcement related to public safety or otherwise relevant to their authorized duties;
- Support local, state, federal, and tribal public safety departments in the identification of subjects associated with/as targets of criminal investigations;
- Support law enforcement response to critical incident responses and special events;
- Support special operations, such as high-crime-area patrols, gang investigation/suppression, operating under the influence initiatives, enforcement details, directed criminal investigations, and other investigations; and
- Support emergency and public safety situations including, but not limited to terrorist threats, kidnappings, missing persons, and felons actively traveling to or from a crime scene.

ALPR Administrator

The Division Commander of Field Services (DFS) shall:

- Designate a 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:

- Ensure the proper selection of personnel approved to operate the ALPR System and maintain an adequate number of trained and authorized users;
- Authorize any requests for ALPR System use or data access according to Department policy;
- Coordinate with all Divisions to ensure resources are available and deployed to meet Departmental investigative needs;
- Ensure 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;
- Designate users who have been properly trained in the use and operational protocols of the ALPR System;
- Allow access to the ALPR System for those users with an approved login and password; and
- Ensure that any changes in hardware, software, policy, or law are the subject of continuing in-service training or bulletins.

ALPR Procedures

The use of ALPR technology shall be approved by the Colonel/Superintendent or designee.

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 members of this Department or by other law enforcement agencies through the ALPR Administrator.

ALPR Operations

Members using the ALPR System shall:

- Ensure, at the start of each shift, 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.

ALPR Alerts/Hits

The member shall, prior to initiation of a stop based on an ALPR Hit or Alert:

- Visually verify that the vehicle plate number matches the plate number run by the ALPR System, including both:
  - Alphanumeric characters of the license plate; and
  - The state of issue.
- Verify the current status of the plate through:
  - The Commonwealth's Criminal Justice Information System (CJIS), or
  - National Crime Information Center (NCIC), or
  - Department's Records Management System (RMS), or
  - Another appropriate source of data, as soon as practicable.

ALPR Alerts/Hits, continued

License plate numbers and date/time location collected through an ALPR, when taken alone, may not be sufficient to identify the individual associated with the vehicle. The Department may be able to link the ALPR information to an individual through, or in combination with, additional information from other sources, such as a check of vehicle registration. It is thus the investigative process that ultimately identifies individuals and not solely a reliance on the information obtained from the ALPR system's automated collection of license plate numbers.

Manual Entry of Data/Manual Hot List

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);
- Investigative needs;
- 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 one (1) year or less.

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.

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;

ALPR Data: Logs, Sharing, Dissemination, and Retention, continued

- 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 and/or intimidating any individual or group;
- Targeting of any individual or group by means of camera placement or data use in a discriminatory manner; and
- Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

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 (i.e., the identity of an individual could be directly or indirectly inferred by using information that is linked or linkable to that individual).

Information 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 point of contact, in writing or electronically, when the Department's ALPR information is alleged, suspected, or found to be erroneous or deficient.

Security

The following shall apply to ALPR system and information security:

- The Department of Criminal Justice Information Services of the Executive Office of Public Safety and Security will operate ALPR servers in a secure facility protected from external intrusion and will utilize secure internal and external safeguards against network intrusions. Any access to DCJIS ALPR information from outside the facility will be allowed only over secure networks;
- The Department and DCJIS will store ALPR information in a manner that ensures that it cannot be added to, modified, accessed, or purged except by personnel authorized to take such actions;
- Access to Department ALPR information will be granted only to personnel whose positions and job duties require such access and who have successfully completed a background check and training;
- Usernames and passwords to ALPR information are not transferrable, must not be shared by Department personnel, and must be kept confidential;
- Queries made to the Department's ALPR information will be logged into the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit; and
- The Department and DCJIS will maintain an audit trail of accessed, requested, or disseminated Department-held ALPR information. The audit trail will be retained for a minimum of one year. It will include all requests for access to ALPR information, the specific purposes for each request, and what ALPR information was disseminated to each individual in response to that request.

State Central Repository

The Department has agreed to:

- Electronically submit captured ALPR data to the state repository maintained by the DCJIS at the Commonwealth's Public Safety Data Center.

The Department and its users agree to the terms of this policy and to the Commonwealth of Massachusetts *Global Justice and Public Safety Information Sharing Policy* of the DCJIS.

Policy Review

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.

Because existing technology may progress and new technology may develop, giving rise to both legal and technological issues, the Department will monitor and assess the appropriateness of this policy, and make amendments as necessary.

References: Executive Office of Public Safety and Security (EOPSS) – The Commonwealth of Massachusetts Global Justice and Public Safety Information Sharing Policy;
EOPSS – Department of Criminal Justice Information Services – Automatic License Plate Recognition System Central Repository Companion Policy;
MPAC: 41.3.9.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
January 22, 2021	**TRF-11**

Subject:

Automatic License Plate Recognition

Policy

The availability and use of the Automatic License Plate Recognition (ALPR) System provides opportunities for enhancing the productivity and effectiveness of law enforcement agencies. The ALPR System also provides opportunities to increase public and officer safety.

The 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.

Purpose

To establish guidelines and procedures for the proper use and application of the ALPR System within the Department of State Police, and to provide guidelines and principles for the collection, access, use, dissemination, and retention of ALPR information by members 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.

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 through, utilization of the ALPR System.

ALPR Data Query Logs: A record of a search or query of ALPR data.

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.

Continued on next page

Definitions and Acronyms (Continued)

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, Incapacitated or Endangered Persons, 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.

Authorized Uses

The provisions of this policy are provided to support authorized uses of ALPR information. Authorized uses may include, but are not limited to, the following:

- Investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime;
- Enhance Department's AMBER/SILVER or other law enforcement alerts and real-time response capability by deploying and networking ALPRs across the state to more rapidly identify and locate vehicles related to potential child-abduction or other serious crimes;
- Alert law enforcement that a particular license plate on a "hot list" (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 and assist in locating dangerous and wanted individuals;
- Identify plates associated with potential witnesses and/or victims of crime;
- Support the Department's homeland security mission by protecting critical infrastructure from subjects who intend to damage or disrupt the systems and locations that allow for travel and the free flow of commerce;

Continued on next page

Authorized Uses, continued

- Identify vehicles linked to stolen license plates or other motor vehicle traffic violations;
- Provide situational awareness for law enforcement related to public safety or otherwise relevant to their authorized duties;
- Support local, state, federal, and tribal public safety departments in the identification of subjects associated with/as targets of criminal investigations;
- Support law enforcement response to critical incident responses and special events;
- Support special operations, such as high-crime-area patrols, gang investigation/suppression, operating under the influence initiatives, enforcement details, directed criminal investigations, and other investigations; and
- Support emergency and public safety situations including, but not limited to terrorist threats, kidnappings, missing persons, and felons actively traveling to or from a crime scene.

ALPR Administrator

The Division Commander of Field Services (DFS) shall:

- Designate a 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:

- Ensure the proper selection of personnel approved to operate the ALPR System and maintain an adequate number of trained and authorized users;
- Authorize any requests for ALPR System use or data access according to Department policy;
- Coordinate with all Divisions to ensure resources are available and deployed to meet Departmental investigative needs;
- Ensure 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;
- Designate users who have been properly trained in the use and operational protocols of the ALPR System;
- Allow access to the ALPR System for those users with an approved login and password; and
- Ensure that any changes in hardware, software, policy, or law are the subject of continuing in-service training or bulletins.

Continued on next page

ALPR Procedures

The use of ALPR technology shall be approved by the Colonel/Superintendent or designee.

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 members of this Department or by other law enforcement agencies through the ALPR Administrator.

ALPR Operations

Members using the ALPR System shall:

- Ensure, at the start of each shift, 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.

ALPR Alerts/Hits

The member shall, prior to initiation of a stop based on an ALPR Hit or Alert:

- Visually verify that the vehicle plate number matches the plate number run by the ALPR System, including both:
  - Alphanumeric characters of the license plate; and
  - The state of issue.
- Verify the current status of the plate through:
  - The Commonwealth's Criminal Justice Information System (CJIS), or
  - National Crime Information Center (NCIC), or
  - Department's Records Management System (RMS), or
  - Another appropriate source of data, as soon as practicable.

Continued on next page

ALPR Alerts/Hits

License plate numbers and date/time location collected through an ALPR, when taken alone, may not be sufficient to identify the individual associated with the vehicle. The Department may be able to link the ALPR information to an individual through, or in combination with, additional information from other sources, such as a check of vehicle registration. It is thus the investigative process that ultimately identifies individuals and not solely a reliance on the information obtained from the ALPR system's automated collection of license plate numbers.

Manual Entry of Data/Manual Hot List

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);
- Investigative needs;
- 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 one (1) year or less.

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.

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;

Continued on next page

ALPR Data: Logs, Sharing, Dissemination, and Retention, continued

- 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 and/or intimidating any individual or group;
- Targeting of any individual or group by means of camera placement or data use in a discriminatory manner; and
- Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

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 (i.e., the identity of an individual could be directly or indirectly inferred by using information that is linked or linkable to that individual).

Information 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 point of contact, in writing or electronically, when the Department's ALPR information is alleged, suspected, or found to be erroneous or deficient.

Continued on next page

Security

The following shall apply to ALPR system and information security:

- The Department of Criminal Justice Information Services of the Executive Office of Public Safety and Security will operate ALPR servers in a secure facility protected from external intrusion and will utilize secure internal and external safeguards against network intrusions. Any access to DCJIS ALPR information from outside the facility will be allowed only over secure networks;
- The Department and DCJIS will store ALPR information in a manner that ensures that it cannot be added to, modified, accessed, or purged except by personnel authorized to take such actions;
- Access to Department ALPR information will be granted only to personnel whose positions and job duties require such access and who have successfully completed a background check and training;
- Usernames and passwords to ALPR information are not transferrable, must not be shared by Department personnel, and must be kept confidential;
- Queries made to the Department's ALPR information will be logged into the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit; and
- The Department and DCJIS will maintain an audit trail of accessed, requested, or disseminated Department-held ALPR information. The audit trail will be retained for a minimum of one year. It will include all requests for access to ALPR information, the specific purposes for each request, and what ALPR information was disseminated to each individual in response to that request.

State Central Repository

The Department has agreed to:

- Electronically submit captured ALPR data to the state repository maintained by the DCJIS at the Commonwealth's Public Safety Data Center.

The Department and its users agree to the terms of this policy and to the Commonwealth of Massachusetts *Global Justice and Public Safety Information Sharing Policy* of the DCJIS.

Continued on next page

Policy Review

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.

Because existing technology may progress and new technology may develop, giving rise to both legal and technological issues, the Department will monitor and assess the appropriateness of this policy, and make amendments as necessary.

References:

Executive Office of Public Safety and Security (EOPSS) – The Commonwealth of Massachusetts Global Justice and Public Safety Information Sharing Policy
EOPSS – Department of Criminal Justice Information Services – Automatic License Plate Recognition System Central Repository Companion Policy
MPAC: 41.3.9

Promulgated By: Christopher S. Mason, Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
June 27, 2023	**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: License plate numbers of vehicles of interest, such as stolen vehicles or stolen plates, vehicles associated with missing or endangered persons, AMBER & Silver alerts, kidnappings, wanted fugitives, and others of specific interest to law enforcement that have a license plate number associated to them, including 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 managed, purchased, or subscribed to by the Department.

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 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 or locations 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 and operators 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 knowingly 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 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 conduct or authorize training for designated personnel in the use and operational protocols of the ALPR system;
- Coordinate with all Divisions and appropriate personnel to ensure that resources are available and deployed to meet Departmental needs;
- Maintain proficiency and familiarity with ALPR technology and systems, coordinate with other law enforcement agencies, and assist with investigations involving ALPR;
- Ensure that designated, trained personnel install equipment, check equipment 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 coordinate the purchase, deployment, and installation of ALPR systems and equipment;
- Conduct intermittent audits of ALPR system usage to ensure functionality and policy compliance; and
- Ensure that any substantive changes in policy or law are the subject of in-service training or bulletins.

Legal Considerations

In additional to the procedural safeguards outlined by this policy, members should conduct ALPR inquiries in the least intrusive manner as necessary and appropriate for the particular circumstances and should consider consulting with a prosecutor of jurisdiction regarding the potential need for legal process prior to accessing extensive or widespread ALPR data in active criminal investigations that do not involve exigent circumstances. See Commonwealth v. McCarthy, 484 Mass. 493 (2020).

Search Procedures

The Commonwealth Watch Center (CWC) and Commonwealth Fusion Center (CFC) shall serve as the primary ALPR resource for the Department. Search requests submitted to the CWC/CFC shall include, at a minimum:

- Case number or reference;
- Type of investigation or reason for request;
- Plate number(s) and vehicle description (if available);
- Requested search time period; and
- Requested search area (devices or region).

Searches of the ALPR system shall also observe the following guidelines:

- Properly complete justification fields;
- Limit search parameters to be reasonable and consistent with the geographic and temporal needs of the incident or investigation; and
- Document the parameters of the search.

The member who conducts or requests the search is responsible for ensuring that the procedures herein are followed. CWC/CFC may deny or refer to the ALPR Administrator any requests that they believe to be overly intrusive or otherwise inconsistent with law, policy, or best practices.

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, missing person, or kidnapping broadcasts or bulletins;
- Incapacitated or endangered persons;
- Be-On-Look-Out (BOLO) broadcasts or other public safety alerts;
- Investigation of terrorist or criminal offenses; or
- Wanted persons, arrest warrants, or search warrants.

Manual entries onto a Hot List shall be:

- Entered with the vehicle description, if available;
- Entered with a case number or reference;
- Updated or removed when information changes, is no longer current, or is no longer necessary or reasonable;
- Given special attention to rental and short-term use vehicles;
- Given special attention to incidents that may be quickly resolved;
- Entered with an automatic expiration date no longer than thirty (30) days; and
- Approved by a supervisor, except in exigent circumstances.

Manual Hot List Entries, continued

Designated and trained ALPR system users may conduct manual Hot List entries. All others should contact the Commonwealth Watch Center for assistance. The member who enters or requests a manual Hot List entry shall be responsible for ensuring that the information is removed per the guidelines above.

Mobile Operations

Department members operating a cruiser that is equipped with a mobile ALPR System shall:

- Ensure, at the start of each shift, that the ALPR system is activated and online, unless such use is incompatible with the member's duties at the time, the system is malfunctioning, or authorized by a supervisor;
- Ensure, 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

Prior to initiation of a stop or enforcement action based upon an ALPR hit or alert, members shall confirm the hit or alert, to include:

- *Verify the plate:* Visually verify that the vehicle plate matches the ALPR system's 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 that generated the hit/alert (e.g., is the vehicle still stolen), 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 information, records, or data from non-departmental ALPR systems.

Supervisors and analysts assigned to the Commonwealth Watch Center/Commonwealth Fusion Center and the ALPR Administrator may access non-departmental ALPR systems for official law enforcement purposes as authorized by this policy. 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, retention, and quality assurance standards than the Department's ALPR system. Members shall be mindful to preserve, export, or obtain copies of records or reports that are of known relevance to an incident or investigation prior to the expiry of the records.

Requests for Equipment and Accounts

Requests for the deployment or issuance of ALPR equipment or system accounts shall be directed through channels to the ALPR Administrator.

The ALPR administrator will approve, deny, or forward requests for deployment, equipment, and accounts as authorized under this policy, based upon the state-wide needs of the ALPR program, the availability of suitable equipment and personnel, and/or as directed by the Division Commander of Homeland Security and Preparedness.

Data: PII, Sharing, and Retention

License plate numbers and date/time location records collected by 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 or other investigative steps. 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) making a request for official purposes, 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 that are authorized to share data with the Department and/or access the Department's ALPR system shall be subject to the provisions of this policy or any superseding MOU or agreement in regard to use of the Department's ALPR system. Such outside agencies are responsible for their own designation, management, and supervision of that agency's system users, equipment, and any other systems or databases.

The ALPR system does not collect or retain video or audio recordings or intentional photographs of any individuals.

Retention of data shall be determined by the Department of Criminal Justice Information Services (DCJIS) policy. Members shall be mindful to preserve, export, or obtain copies of records or reports that are of known relevance to an investigation or prosecution prior to the expiry of the records.

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 data 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 or legal proceeding.

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 sworn or civilian personnel whose positions and job duties justify such access, who have successfully completed a pre-employment background check, and who have completed appropriate training as designated by the ALPR Administrator, to include discussion of best practices and privacy considerations;
- Usernames and passwords to the ALPR system are not transferrable, must not be shared by Department personnel, and must be kept confidential; the only exception to this requirement is for mobile ALPR systems in pool cruisers in use by outside agencies, in which case the credentials can be used to activate the in-car camera system only and not to access or search the database; in such case the agency must maintain another tracking mechanism to identify the specific system operator, if needed;
- 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 monitoring, review, and audit at any time;
- Abuse of the Department's ALPR system will result in termination of system access and progressive disciplinary action; 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.

Reservations

These guidelines are set forth solely for the purpose of internal Department guidance. They are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter, civil or criminal, nor do they place any limitation on otherwise lawful investigative and legal prerogatives of the Massachusetts State Police or the Commonwealth of Massachusetts.

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
MPAC 41.3.9

Promulgated By: John E. Mawn Jr., Colonel/Superintendent

Department of State Police
General Order

Effective Date:	Number:
November 10, 2021	**TRF-11**
Subject:	
Automatic License Plate Recognition	

Policy

The availability and use of the Automatic License Plate Recognition (ALPR) System provides opportunities for enhancing the productivity and effectiveness of law enforcement agencies. The ALPR System also provides opportunities to increase public and officer safety.

The 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.

Purpose

To establish guidelines and procedures for the proper use and application of the ALPR System within the Department of State Police, and to provide guidelines and principles for the collection, access, use, dissemination, and retention of ALPR information by members 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.

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 through, utilization of the ALPR System.

ALPR Data Query Logs: A record of a search or query of ALPR data.

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.

Definitions and Acronyms, continued

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, Incapacitated or Endangered Persons, 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.

Authorized Uses

The provisions of this policy are provided to support authorized uses of ALPR information. Authorized uses may include, but are not limited to, the following:

- Investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime;
- Enhance Department's AMBER/SILVER or other law enforcement alerts and real-time response capability by deploying and networking ALPRs across the state to more rapidly identify and locate vehicles related to potential child-abduction or other serious crimes;
- Alert law enforcement that a particular license plate on a "hot list" (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 and assist in locating dangerous and wanted individuals;
- Identify plates associated with potential witnesses and/or victims of crime;
- Support the Department's homeland security mission by protecting critical infrastructure from subjects who intend to damage or disrupt the systems and locations that allow for travel and the free flow of commerce;

Authorized Uses, continued

- Identify vehicles linked to stolen license plates or other motor vehicle traffic violations;
- Provide situational awareness for law enforcement related to public safety or otherwise relevant to their authorized duties;
- Support local, state, federal, and tribal public safety departments in the identification of subjects associated with/as targets of criminal investigations;
- Support law enforcement response to critical incident responses and special events;
- Support special operations, such as high-crime-area patrols, gang investigation/suppression, operating under the influence initiatives, enforcement details, directed criminal investigations, and other investigations; and
- Support emergency and public safety situations including, but not limited to terrorist threats, kidnappings, missing persons, and felons actively traveling to or from a crime scene.

ALPR Administrator

The Division Commander of Field Services (DFS) shall:

- Designate a 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:

- Ensure the proper selection of personnel approved to operate the ALPR System and maintain an adequate number of trained and authorized users;
- Authorize any requests for ALPR System use or data access according to Department policy;
- Coordinate with all Divisions to ensure resources are available and deployed to meet Departmental investigative needs;
- Ensure 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;
- Designate users who have been properly trained in the use and operational protocols of the ALPR System;
- Allow access to the ALPR System for those users with an approved login and password; and
- Ensure that any changes in hardware, software, policy, or law are the subject of continuing in-service training or bulletins.

ALPR Procedures

The use of ALPR technology shall be approved by the Colonel/Superintendent or designee.

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 members of this Department or by other law enforcement agencies through the ALPR Administrator.

ALPR Operations

Members using the ALPR System shall:

- Ensure, at the start of each shift, 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.

ALPR Alerts/Hits

The member shall, prior to initiation of a stop based on an ALPR Hit or Alert:

- Visually verify that the vehicle plate number matches the plate number run by the ALPR System, including both:
  - Alphanumeric characters of the license plate; and
  - The state of issue.
- Verify the current status of the plate through:
  - The Commonwealth's Criminal Justice Information System (CJIS), or
  - National Crime Information Center (NCIC), or
  - Department's Records Management System (RMS), or
  - Another appropriate source of data, as soon as practicable.

ALPR Alerts/Hits, continued

License plate numbers and date/time location collected through an ALPR, when taken alone, may not be sufficient to identify the individual associated with the vehicle. The Department may be able to link the ALPR information to an individual through, or in combination with, additional information from other sources, such as a check of vehicle registration. It is thus the investigative process that ultimately identifies individuals and not solely a reliance on the information obtained from the ALPR system's automated collection of license plate numbers.

Manual Entry of Data/Manual Hot List

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);
- Investigative needs;
- 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 one (1) year or less.

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.

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;

ALPR Data: Logs, Sharing, Dissemination, and Retention, continued

- 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 and/or intimidating any individual or group;
- Targeting of any individual or group by means of camera placement or data use in a discriminatory manner; and
- Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

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 (i.e., the identity of an individual could be directly or indirectly inferred by using information that is linked or linkable to that individual).

Information 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 point of contact, in writing or electronically, when the Department's ALPR information is alleged, suspected, or found to be erroneous or deficient.

Security

The following shall apply to ALPR system and information security:

- The Department of Criminal Justice Information Services of the Executive Office of Public Safety and Security will operate ALPR servers in a secure facility protected from external intrusion and will utilize secure internal and external safeguards against network intrusions. Any access to DCJIS ALPR information from outside the facility will be allowed only over secure networks;
- The Department and DCJIS will store ALPR information in a manner that ensures that it cannot be added to, modified, accessed, or purged except by personnel authorized to take such actions;
- Access to Department ALPR information will be granted only to personnel whose positions and job duties require such access and who have successfully completed a background check and training;
- Usernames and passwords to ALPR information are not transferrable, must not be shared by Department personnel, and must be kept confidential;
- Queries made to the Department's ALPR information will be logged into the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit; and
- The Department and DCJIS will maintain an audit trail of accessed, requested, or disseminated Department-held ALPR information. The audit trail will be retained for a minimum of one year. It will include all requests for access to ALPR information, the specific purposes for each request, and what ALPR information was disseminated to each individual in response to that request.

State Central Repository

The Department has agreed to:

- Electronically submit captured ALPR data to the state repository maintained by the DCJIS at the Commonwealth's Public Safety Data Center.

The Department and its users agree to the terms of this policy and to the Commonwealth of Massachusetts *Global Justice and Public Safety Information Sharing Policy* of the DCJIS.

Policy Review

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.

Because existing technology may progress and new technology may develop, giving rise to both legal and technological issues, the Department will monitor and assess the appropriateness of this policy, and make amendments as necessary.

References: Executive Office of Public Safety and Security (EOPSS) – The Commonwealth of Massachusetts Global Justice and Public Safety Information Sharing Policy;
EOPSS – Department of Criminal Justice Information Services – Automatic License Plate Recognition System Central Repository Companion Policy;
MPAC: 41.3.9.

Promulgated By: Christopher S. Mason, Colonel/Superintendent

AGREEMENT BETWEEN AGENCIES

Automatic License Plate Recognition (ALPR) Equipped Law Enforcement Agencies

FOR SHARING LAW ENFORCEMENT INFORMATION

I. OVERVIEW

a. Introduction:

The purpose of this "Agreement" is to outline conditions under which the Agency Parties will share and use "scanned plate" and "hotlist" information. This Agreement is meant to be a "single sign on" agreement where there are multiple Agency Parties but an Agency Party can pick any or all Agency Parties with which to share data.

b. Background:

Automatic License Plate Recognition (ALPR) is a computer-based system that utilizes emerging technology to capture a color image, as well as an infrared image, of the license plate of a vehicle. The infrared image is converted into a text file utilizing Optical Character Recognition (OCR) technology. The text file is automatically compared against an "informational data file," also known as a "hotlist," and can contain information on stolen or wanted vehicles as well as vehicles associated with Amber Alerts, warrant subjects, and agency defined-information.

ALPR cameras can be mobile (mounted on vehicles) or on fixed positions such as freeway overpasses or traffic signals. ALPR systems have all the necessary equipment to scan plates, notify the user of a vehicle hit, and upload the scanned plate information into an ALPR repository for retention and research.

The Agency entering into this Agreement hereinafter referred to as "Agency Party," realizing the mutual benefits to be gained by sharing information, seek to share scanned plate and hotlist information. The specific technological means for securely connecting these informational sources will be approved by agency ALPR administrators.

II. AUTHORIZED RELEASE OF INFORMATION

a. Sharing of Information:

Each Agency Party authorizes the release of scanned plate and hotlist information residing in their respective databases or networks to other Agency Parties as permitted by law. An Agency Party that does not want certain information made available to any other Agency Party is responsible for ensuring that the information is not available for data exchange. There is no obligation to share scanned plate or hotlist information with any Agency Parties based solely on their acceptance of this Agreement.

b. Limitation on Information Sharing:

Scanned plate and hotlist information shall only be shared with or released to other Agency Parties. Only authorized employees who have an approved login and password ("Authorized Users"), and a need and/or right to know, will be allowed to access any other Agency Party's scanned plate and hotlist information.

c. Liability:

Each Agency Party is solely responsible for any and all claims (including, without limitation, claims for bodily injury, death, or damage to property), demands, obligations, damages, actions, causes of action, suits, losses, judgements, fines, penalties, liabilities, costs and expenses (including, without limitation, attorney fees, disbursements and court costs), and claims of every kind and nature whatsoever, arising in any manner by reason of the negligent acts, errors, omissions, or willful misconduct incident to the performance of this Agreement, including the use or alleged or actual misuse of scanned plate and hotlist information by that Party, its officers, agents or employees, this is to include data breaches.

III. INFORMATION OWNERSHIP

a. Ownership:

Each Agency Party retains control of all information in its ALPR repository. Each Agency Party is responsible for creating, updating, and deleting records in its own repository according to its own retention policies. Each Agency Party shall use reasonable efforts to ensure the completeness and accuracy of its data.

b. Release of Information:

Agency Parties and authorized users shall release or make available information accessed from an ALPR repository only to persons or entities authorized to receive ALPR information.

c. Unauthorized Requests:

If an Agency Party receives a request for information in an ALPR repository by anyone who is not authorized to receive information from the ALPR repository, that Agency Party shall refer the request to the law enforcement agency that originated the requested information ("Source Agency").

d. Public Record Requests, Subpoenas, and Court Orders:

Any Agency Party receiving a public records request, subpoena, or court order ("Legal Request") for information in an ALPR repository not authored by or originated by that Agency Party shall immediately provide a copy of the Legal Request to the Source Agency, prior to providing a response to the Legal Request.

IV. UNDERSTANDING ON ACCURACY OF INFORMATION

a. Accuracy of Information:

Agency Parties agree that scanned plate and hotlist information consists of information assumed to be accurate. Agency Parties will participate in routine testing sessions to validate and ensure that its information is accurate. However, data inaccuracies can arise for multiple reasons (e.g., entry errors, misinterpretation, outdated data, etc.). It shall be the responsibility of the Agency Party requesting or using the data to confirm the accuracy of the information with the Source Agency prior to taking any enforcement-related action.

b. Timeliness of Hotlist Data:

Each Agency Party shall determine the frequency with which its hotlist data will be refreshed. Since changes or additions to hotlist data do not get updated on a real-time basis, Agency Parties recognize that information may not always be timely and relevant. It shall be the responsibility of the requesting Agency Party to confirm the timeliness and relevance of the information with the Source Agency. Additionally, a data refresh schedule will be made available by each system administrator to enable a user to determine the potential timeliness of each Agency Party's data. Agency Parties shall not store shared hotlist data on any system for more than a 24-hour period without refreshing it.

V. USER ACCESS

a. Login Application Process:

Each Agency Party's system administrator is responsible for management of user accounts at that Agency Party. Each Agency Party agrees that all authorized users shall be limited to current employees who are legally authorized to review criminal history data for crime prevention and detection purposes. Each potential user shall submit a request for a login and password to the Agency system administrator. The Agency system administrator shall have discretion to deny or revoke individual access.

b. Login Assignment:

Each Authorized User will be issued a user login and a default password by the Agency system administrator. Authorized Users may be assigned to groups that have different levels of access rights based on the level of restriction of the information.

c. Termination of Logins:

Each Agency system administrator is responsible for timely removal of any login accounts as Authorized Users leave the Agency, no longer qualify for access into the system, or are denied access by the Agency system administrator for any other reason.

d. Intended Use:

Each Authorized User agrees that scanned plate, hotlist information, and the networking resources are to be used solely for law enforcment purposes only and consistent with the law. Authorized Users shall not use or share the information for any unethical, illegal, criminal, or commercial purpose.

e. Limitations of Use of Logins:

An Authorized User shall not access information in an ALPR repository by using a name or password that was assigned to another user. An Authorized User shall not give his or her password to another person, including another user, to access the system.

f. Audit Trail:

Each transaction on an ALPR repository is to be logged, and an audit trail created. Each Agency system administrator shall conduct an internal audit on a periodic basis to ensure information is reasonably up to date and user queries are made for legitimate law enforcement purposes only. This information shall be recorded and retained to allow the system administrator to complete the internal audit. Each system administrator shall maintain the audit trail pursuant to the retention policies of that Agency Party. Requests for transaction logs shall be made in writing to the Agency system administrator, who shall provide the logs to the requesting party within a reasonable amount of time.

VI. CONFIDENTIALITY OF INFORMATION

a. Information Confidentiality:

Information in an ALPR repository is confidential and is not subject to public disclosure, except as required by law. Only Authorized Users are allowed to view and use the information in an ALPR repository. Otherwise, the information shall be kept confidential.

b. Internal Requests for Information:

An Authorized User who receives a request from a non-authorized requestor for information in an ALPR repository shall not release that information, but may refer the requestor to the Source Agency.

c. Removal or Editing of Records:

Agency Parties shall determine their own schedule for record deletion and other edits to their own data. This will be determined by policy, legal requirements, storage, and technical capability.

VII. SYSTEM ACCESS

a. Network Access:

Access to scanned plate and hotlist information will be provided via such method that is mutually acceptable to the Agency Parties.

b. System Availablility:

ALPR repositories shall operate 24 hours a day, seven days a week, with downtime limited to those hours required for any necessary maintenance activities.

VIII. AGREEMENT TERMS

a. Term:

This Agreement will commence on the date that it is executed by all Agency Parties. It will terminate only as allowed by Section IX.

b. Amendments:

Any change in the terms of this Agreement shall be incorporated into this Agreement by a written amendment properly executed and signed by the person authorized to bind the Agency Parties.

c. Controlling Law and Venue:

Any dispute that arises under or relates to this Agreement (whether contract, tort, or both) shall be adjudicated according to the laws of the State of California.

d. Severability:

If any term or portion of this Agreement is held to be invalid, illegal, or otherwise unenforceable by a court of competent jurisdiction, the remaining provisions of this Agreement shall continue in full force and effect.

IX. TERMINATION

Either Agency Party to this Agreement may terminate this Agreement upon giving the other Agency Party at least ten (10) days written notice prior to the effective date of such termination, which date shall be specified in such notice.

X. SIGN-OFF ON EXECUTION OF AGREEMENT

By executing this Agreement, each Party acknowledges that it has received a copy of this Agreement, and will comply with its terms and conditions. The person executing this Agreement certifies that the person is authorized by its Party to execute this Agreement and legally bind its Party to the terms herein. This Agreement may be executed in one or more counterparts, each of which will be deemed an original, but all of which together will constitue one and the same instrument.

Agency Ventura County Sheriff's Office

Signature: 

Name: Jim Fryhoff

Title: Sheriff

Date: 1-5-2023

Agency Massachusetts State Police

Signature: _____

Name: _____

Title: _____

Date: _____

MANUFACUTRES HARDWARE WARRANTY AGREEMENT

Intelligent Enclosure Product Line

I. AGREEMENT OVERVIEW

This warranty document outlines the standard terms and conditions for the hardware warranty for the Vetted Security Solutions Intelligent Enclosure series of products. The models covered through this warranty include (but are not always limited to):

1) VSS-LPR-MAIN
2) VSS-LPR-BRG
3) VSS-SOLAR-MAIN
4) VSS-CCTV-MAIN
5) VSS-CCTV-LPR-MAIN

The Vetted Solutions enclosure line is manufactured in Saint Petersburg, FL using an E-Verified work force. Vetted Solutions Intelligent Enclosures are the industry leader in terms of both quality and warranty coverage provided with the Enclosure Units. The Vetted Intelligent Enclosure series is covered by a complete component level warranty of 12 months (1 year).

Each component on the tray is tracked to primary enclosure serial number. In the event of a failure, a complete replacement tray preprogrammed to your account specifications. This makes plug and play replacement possible and mitigates long term service cost as well as serves to mitigate downtime in the event of failures.

During this warranty period Vetted Security Solutions LLC (Vetted) warrants to the original end user that each product of its manufacture is free from defects in material and workmanship if properly installed, serviced, and operated under normal conditions.

Vetted's obligation under this warranty is limited to correcting without charge at its factory any part or parts thereof which shall be returned to its factory prepaid within 12 months after purchase by the original user, and which upon examination shall disclose to Vetted's satisfaction to have been originally defective.

This warranty shall not apply to any Vetted product that must be replaced because of normal wear, that has been subject to misuse, negligence, or accident, or that has been

repaired or altered outside of Vetted's factory unless authorized by Vetted personnel in writing.

Vetted makes no warranties with respect to, camera optics, pole infrastructure (when customer supplied pole), or other component parts or accessories not manufactured by Vetted, same being subject only to such warranties, if any, as may be made by their respective manufacturers. Vetted does warrant that it will put forth reasonable effort on behalf of the original users of its products to assure that such manufacturers' warranties are satisfactorily performed.

Use on any Vetted product of replacement parts other than Vetted-certified replacement parts purchased through Vetted or an authorized Vetted distributor shall void this warranty.

THIS WARRANTY, AND VETTED'S OBLIGATION HEREUNDER, IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, and all other obligations or liabilities including special or consequential damages or contingent liabilities arising out of the failure of any product or part to operate properly.

Vetted shall not be liable for any special, indirect, incidental, or consequential damages whether in contract, tort, under any warranty, or otherwise, beyond the warranty quoted herein for products or parts.

No person is authorized to give any other warranty or to assume any additional obligation on Vetted's behalf unless made in writing and signed by an officer of Vetted.

This warranty, dated December 2021, supersedes all prior and undated warranty statements, except statements authorized by Vetted in individual contracts.

II. DURING THE SERVICE / WARRANTY PERIOD

- **a.** Vetted Security Solutions provides standard support line available at 727-440-3245, excluding legal holidays. A 24-hour support ticket system is available at https://vettedsecuritysolutions.com/support/and allows users to create a ticket automatically which will give send you an email you're your ticket number allowing you to track the status of your issue and view tech responses.
- **b.** Vetted Security Solutions will diagnose the issue and provide analysis of cause of issue within a 72-hour period of being notified of issue if trailer unit is still online. If trailer is left offline or inoperable it is the agency POC responsibility to leave time in ticket, phone message, or with technician when remote access can be made available to troubleshoot downed unit.

c. Vetted Security Solutions will provide a maximum fourteen (14) day turn-a-round on repairs from the date of receipt of the item in back to headquarters in Saint Petersburg, FL. Attention should be Vetted Security Solutions RMA Number with reference number for service ticket.

d. Vetted Security Solutions will assure that repairs are completed within specifications with OEM parts.

e. Repaired equipment to have complete warranty for 6-month period or original warranty period whichever is longer. Warranty to start at agency's receipt of repaired equipment. Shall include all labor and parts.

f. This warranty does not cover vandalism or units that have been physically damaged in any way.

g. All enclosures will come with QR code sticker with links to documentation, support information, and RMA forms.

III. MAINTENANCE AND SHIPPING

a. All shipping charges to get equipment to Vetted Solutions designated address are the responsibility of agency or partner. Vetted Solutions will cover return shipping cost of any approved warranty return.

b. Software maintenance includes free access to software updates and software hot fixes. Includes updates / patches to software at quarterly increments. Instructions for updates in house to server / client software will also be provided to the agency

SUPPORT CALL PROCESS

For technical support the customer should call the Vetted Security Solutions office number at (727) 440-3245 and then dial 1. This will take you direct to our Service desk.

Another option for support is to create a service ticket through our website. Those steps are outlined below:

1) Go to https://vettedsecuritysolutions.com/support

2) Choose tech support

3)Choose technical support

4) Provide a summary and description of the issue you are having, and we will have record of the ticket in our system.

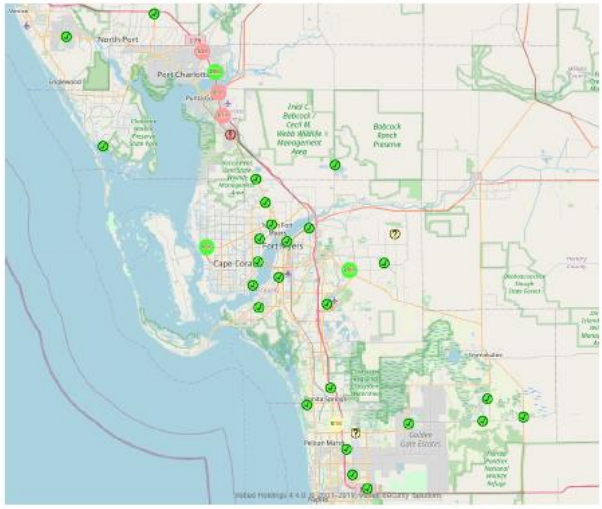
5) Once the ticket is closed it will send you an email notifying you that has been done.

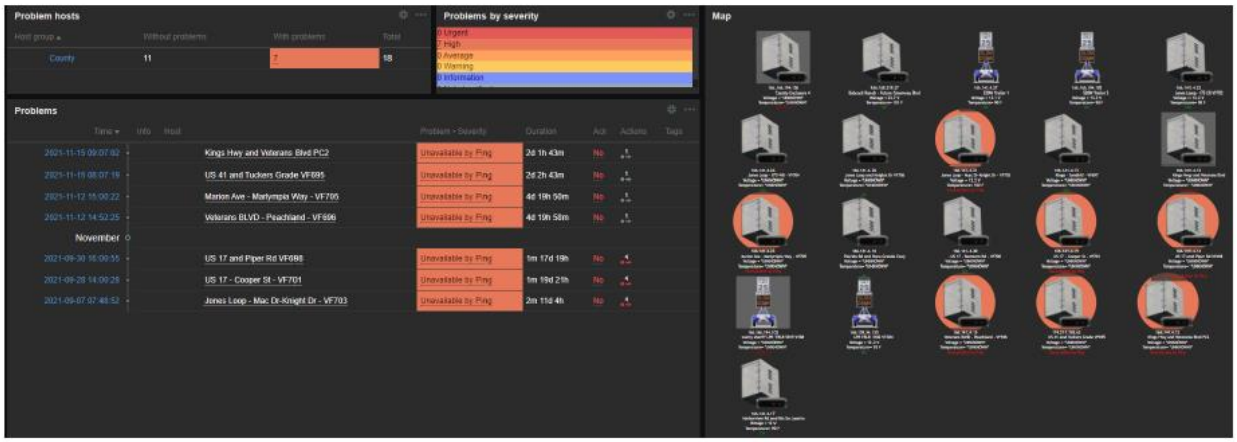
REMOTE SUPPORT TOOL

Some support calls require further analysis of the client's database, process or setup to diagnose a problem or to assist with a question. Vetted Security Solutions will, at its discretion, use an industry-standard remote support tool. Support can quickly connect to the client's desktop and view the site's setup, diagnose problems, or assist with screen navigation. More information about the remote support tool that Vetted Security Solutions uses is available upon request.

Please contact support@vettedsecuritysolutions.com for more information regarding remote support capabilities or sales@vettedsecuritysolutions.com for inquiries on adding Vetted Virtual Technician (VVT) to your agencies support procedures.

VVT is optional add on that allows agency managers and power users to view all deployed equipment, receive alerts, have automated corrective actions taken in event of field level issues, and a host of other customizable features. Screenshot of map interface and dashboard overview included below:







CERTIFICATE OF TRAINING

THIS CERTIFICATE IS PROUDLY PRESENTED TO

Brian.Brooks9

FOR THE SUCCESSFUL COMPLETION OF

VIGILANT VEHICLEMANAGER 101

on Jul 02, 2023

1 Hour

PRESENTED BY

Marcia Broderick

Marcia Broderick
Director, Customer Training and Development

MOTOROLA SOLUTIONS



VIGILANT PLATESEARCH
ACTIVE HIT PROTOCOL

Active Hit Protocol is a step-by-step guideline to ensure you are reacting correctly to a detected license plate alert.

WARNING: Active Hit Protocol should be used every time an alert or hit is received.

STEP ONE

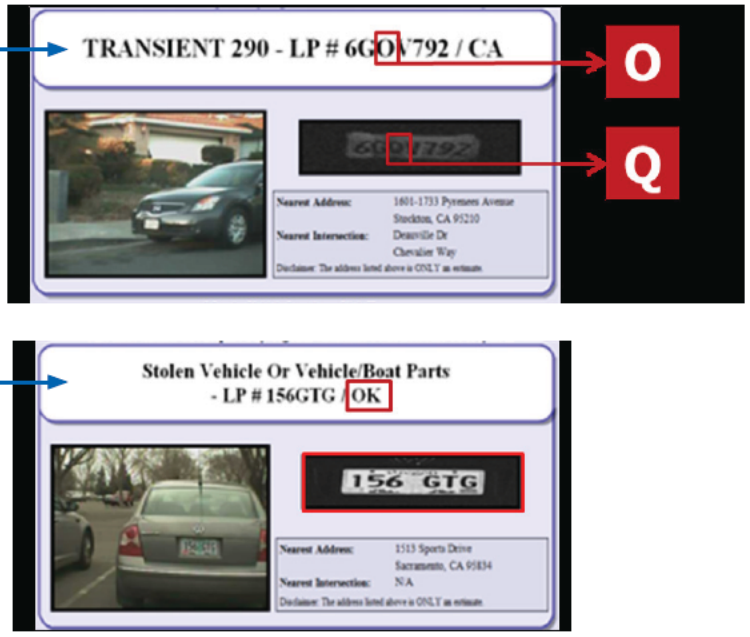
Compare the detection to the translation and check for misreads.

STEP TWO

Confirm the state of the hot list source to the scanned plate.

STEP THREE

Conduct a records check on the plate and ensure it is wanted and in the system.



For further questions or training, please email
VigilantTraining@motorolasolutions.com

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. 11-2020

END OF TRAINING - QUESTIONS?

SAM PALMER

Manager, Client Relations, PS
North Central – US
(480) 549-2901
sam.palmer@motorolasolutions.com

DAVID RIVERA

Manager, Client Relations, PS
Southeast Region – US
(813) 460-6993
david.rivera1@motorolasolutions.com

CHRIS SCANDOLE

Manager, Client Relations, PS
Central Region – US
(917) 913-3351
christopher.scandole@motorolasolutions.com

CHRIS PITTMAN

Manager, Client Relations, PS
South Central – US
(469) 712-3060
chris.pittman@motorolasolutions.com

LEE YONEMURA

Manager, Client Relations, PS
West Coast – US
(916) 307-0893
lee.yonemura@motorolasolutions.com

MARCIA BRODERICK Director, Client Relations Nationwide (279) 201-4142 marcia.broderick@motorolasolutions.com

VIGILANT TRAINING TEAM

VigilantTraining@motorolasolutions.com

Please send us your software update ideas and success stories. **THANK YOU AND STAY SAFE.**

MOTOROLA SOLUTIONS



CERTIFICATE OF TRAINING

THIS CERTIFICATE IS PROUDLY PRESENTED TO

Brian.Brooks9

FOR THE SUCCESSFUL COMPLETION OF

VIGILANT VEHICLEMANAGER INTRODUCTION & USER ACCOUNT MANAGEMENT

on Jul 02, 2023
30 Minutes

PRESENTED BY

Marcia Broderick

Marcia Broderick
Director, Customer Training and Development

MOTOROLA SOLUTIONS



CERTIFICATE OF TRAINING

THIS CERTIFICATE IS PROUDLY PRESENTED TO

Sean.Bender7

FOR THE SUCCESSFUL COMPLETION OF

VIGILANT VEHICLEMANAGER 101

on Jul 02, 2023

1 Hour

PRESENTED BY

Marcia Broderick

Marcia Broderick
Director, Customer Training and Development

MOTOROLA SOLUTIONS



CERTIFICATE OF TRAINING

THIS CERTIFICATE IS PROUDLY PRESENTED TO

Sean.Bender7

FOR THE SUCCESSFUL COMPLETION OF

VIGILANT VEHICLEMANAGER INTRODUCTION & USER ACCOUNT MANAGEMENT

on Jul 02, 2023
30 Minutes

PRESENTED BY

Marcia Broderick

Marcia Broderick
Director, Customer Training and Development

MOTOROLA SOLUTIONS



COVERT SURVEILLANCE ENCLOSURES

VETTED'S COVERT ENCLOSURES ARE THE IDEAL WAY TO GATHER LPR OR VIDEO SURVEILLANCE DATA SIMPLY AND DISCREETLY. EASY TO USE AND NEARLY IMPOSSIBLE TO DETECT.

Gather data with subtly using the latest technology with Vetted's Covert Enclosures.

Featuring concealed sensors, plexiglass windows, internal batteries, and more to create a camouflaged data capture system designed to look like common infrastructure components and blend into the surroundings. Designed for special operations this series offers devices that can be quickly deployed and retrieved for short-duration missions and fixed-mounted devices for long-term operations. These complete surveillance systems include an onboard processor, modem, camera, and more for accurate day and night captures in all-weather environments providing you with essential intelligence.

Advanced ALPR

Powered by Vigilant LEARN, Vetted's covert solutions provide high-performance license plate scanning with Optical Character Recognition and OptimizedIR. These systems are designed to capture plate images day or night, across multiple lanes, and at various speeds.

Configured for Valuable Analytics

Custom hotlists, real-time alerts, and comprehensive search and report capabilities are just a few of the valuable analytics included with Vetted's ALPR camera systems. Create and share hotlists with other agencies and download data from national databases such as NCIC to close more cases.

Ready to Deployment

Vetted's robust covert camera systems are ready for permanent or temporary deployments. With features like rapid installation, quick-connect power, and rapid positioning the covert family of products delivers functional performance and options to match the mission.

CUSTOMIZED UTILITY BOX

This enclosure is designed to blend in with common street-side traffic and electrical cabinets. The interior contains a positionable camera, modem, and video processor. These systems can be deployed quickly and are designed for short and long term missions.



	UTILITY BOX ENCLOSURE	
Part #	VSS-CVRT-UTILITY-ENC-850	VSS-CVRT-UTILITY-ENC-940
Highlighted Features	• Axis Q1700-LE camera with long-range optimized IR • HD 1080p with 32x optical zoom • 850nm or 940nm custom IR camera ring • Covers 2 lanes at distances of 66-328 ft • 155 mph max capture speed • Vigilant LEARN software with LINC • Axis Lightfinder 2.0	• Quick-swappable mount for Sierra Wireless RV50/RV55 modem with permanent MIMO antenna • Internal power cable routing with quick disconnect • 120V AC to 24V 10amp power supply • Rugged PoE switch • Vetted Virtual Technician ready
Dimensions (L X W X H)	8.75 in x 12.5 in x 14.25 in	

5G CELLULAR NODE ENCLOSURE

Designed to look like a common cellular pole top antenna. This enclosure features a compact polymer exterior concealing the purpose-built aluminum skeleton that supports the surveillance electronics. These systems are designed for long term deployments.



	CUSTOM MADE 5G ANTENNA ENCLOSURE	
Part #	VSS-CVRT-5G	
Highlighted Features	• Axis Q6135-LE PTZ camera • HD 1080p with 32x optical zoom • Long-range optimized custom 940nm IR • Video capture range up to 820 ft • Covers 2 lanes at distances of 66-328 ft • 155 mph max capture speed • Vigilant LEARN software with LINC • Autotracking 2 with orientation aid • Axis Lightfinder 2.0 • Axis object analytics	• Tycon web monitor • Quick-swappable mount for Sierra Wireless RV50/RV55 modem with permanent MIMO antenna • Internal power cable routing with quick disconnect • 120V AC to 24V 10amp power supply • Rugged PoE switch • Vetted Virtual Technician ready
Dimensions*	22.5 in x 13.5 in	

*Antenna enclosure size without mount arm. Total size with mount arm is 33.5 in x 21.5 in.

CONTACT US TODAY

727.440.3245 sales@vettedsecuritysolutions.com

VETTEDSECURITYSOLUTIONS.COM

VETTED SECURITY SOLUTIONS

© 2022 Vetted Security Solutions. All Rights Reserved. Revised 07.2022



VETTED VIRTUAL TECHNICIAN

MINIMIZE TRIAGE AND ON-SITE VISITS AND SEAMLESSLY MONITOR THE HEALTH OF IP CONNECTED ALPR, CCTV CAMERAS, AND OTHER DEVICES ONLINE.

Vetted Virtual Technician (VVT) powered by FINDER Software Solutions is a web-based application that allows system administrators and authorized users to view the current status and health of their IP connected ALPR, surveillance, and communications equipment in the field.

Whether you have fixed or trailer-mounted systems, VVT monitors all the key hardware and software components of your security intelligence portfolio. This includes each system's power supply, battery, solar recharging performance, CPU, modem, and network communication.

Self-Corrective Steps

VVT automatically resolves common issues that would normally require a field visit, through its self-corrective capabilities.

Multi-Channel Alerts

Alert emails and text messages can be sent to multiple agency administrators when a problem or specific trigger event occurs.

Full Customization

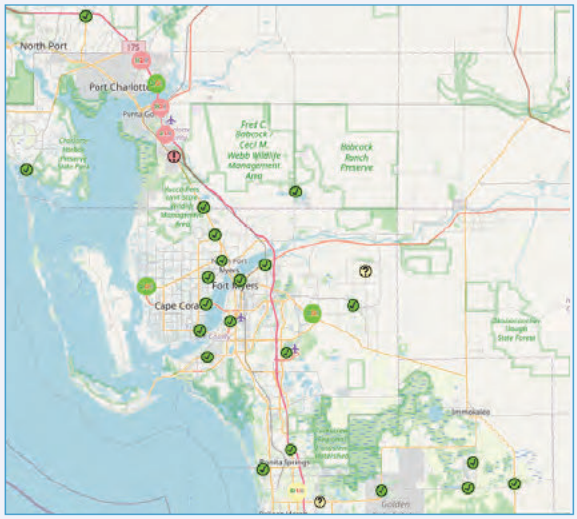
This solution supports unusual and non-standard devices along with customizable alert settings and corrective measures.

ALERT, SO YOU ARE ALWAYS AWARE

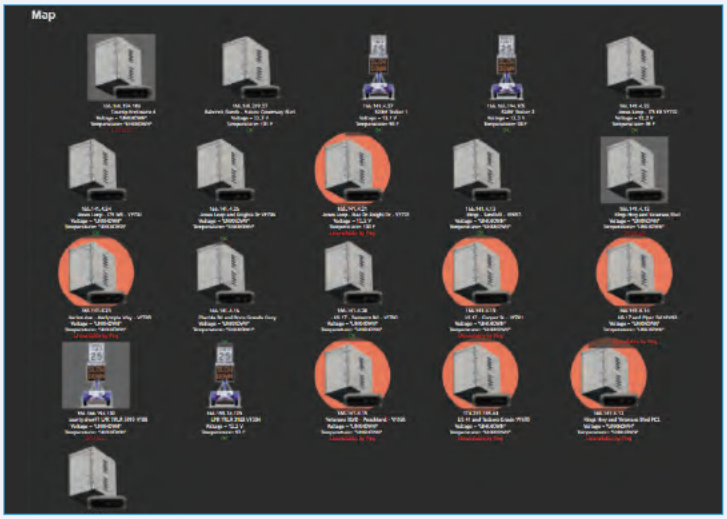
Vetted Virtual Technician is an online tool that monitors the health of all of your field hardware devices in a single, simple-to-use interface.

This includes license plate readers, CCTV cameras, wireless radios, trackers, and other IP connected devices that allow for an automated triaged support response and rebooting. The system can run self-corrective steps to automatically resolve common issues that would normally require a field visit. VVT can also be customized to monitor unusual and non-standard devices. Alert emails and text messages can be sent to multiple agency administrators when a problem or specific trigger event occurs to accelerate corrective action.

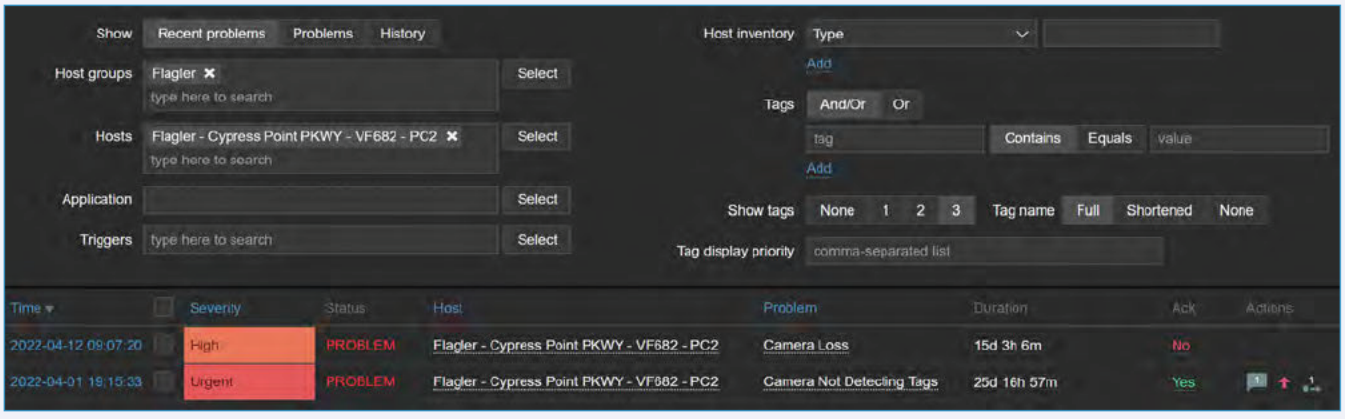
VVT IN ACTION



Site Map provides a visual representation of all monitored sites.



Site Dashboard provides snapshot of all monitored sites and relevant information.



Alert Dashboard provides detailed informtion concerning a problem or trigger event.

CONTACT US TODAY

727.440.3245 sales@vettedsecuritysolutions.com

VETTEDSECURITYSOLUTIONS.COM

VETTED SECURITY SOLUTIONS

© 2022 Vetted Security Solutions. All Rights Reserved. Revised 11.2022

VETTED
SECURITY SOLUTIONS

MINIMIZE TRIAGE AND ON-SITE VISITS WITH VETTED VIRTUAL TECHNICIAN

Seamlessly monitor the health of IP LPR, CCTV cameras, and other devices online.



SELF-CORRECTIVE STEPS

VVT automatically resolves common issues that would normally require a field visit, through its self-corrective capabilities.

FULL CUSTOMIZATION

The solution can also be customized to monitor unusual and non-standard devices.

MULTI-CHANNEL ALERTS

Alert emails and text messages can be sent to multiple agency administrators when a problem or specific trigger event occurs.

ABOUT VETTED VIRTUAL TECHNICIAN

Vetted Virtual Technician (VVT) is a web-based software application that allows law enforcement personnel to view the current status of their in-field ALPR equipment and server communications. Whether you have fixed or trailer-mounted systems, VVT monitors all the key hardware/software components of your ALPRs 24/7. This includes each system's power supply, CPU, cell phone router, internet connectivity, and network communication.

SCHEDULE A DEMO

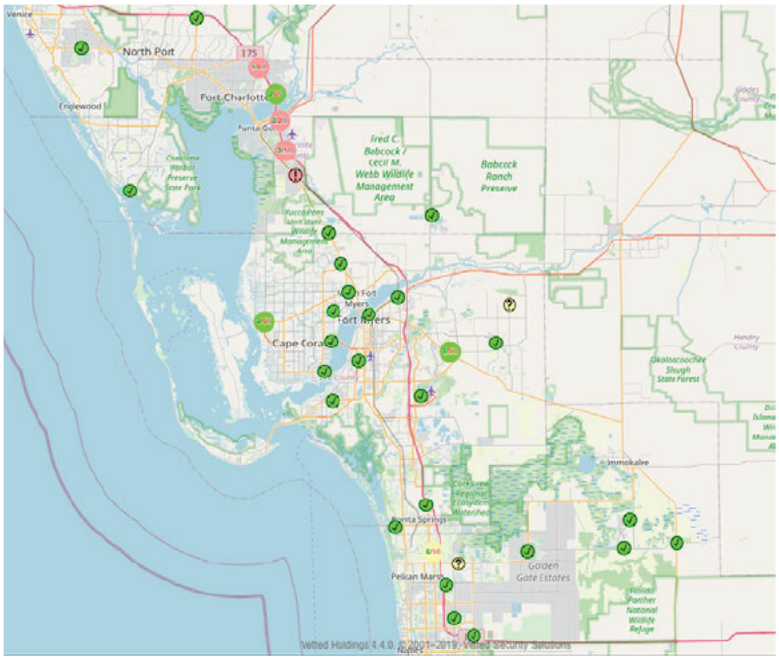
727-440-3245

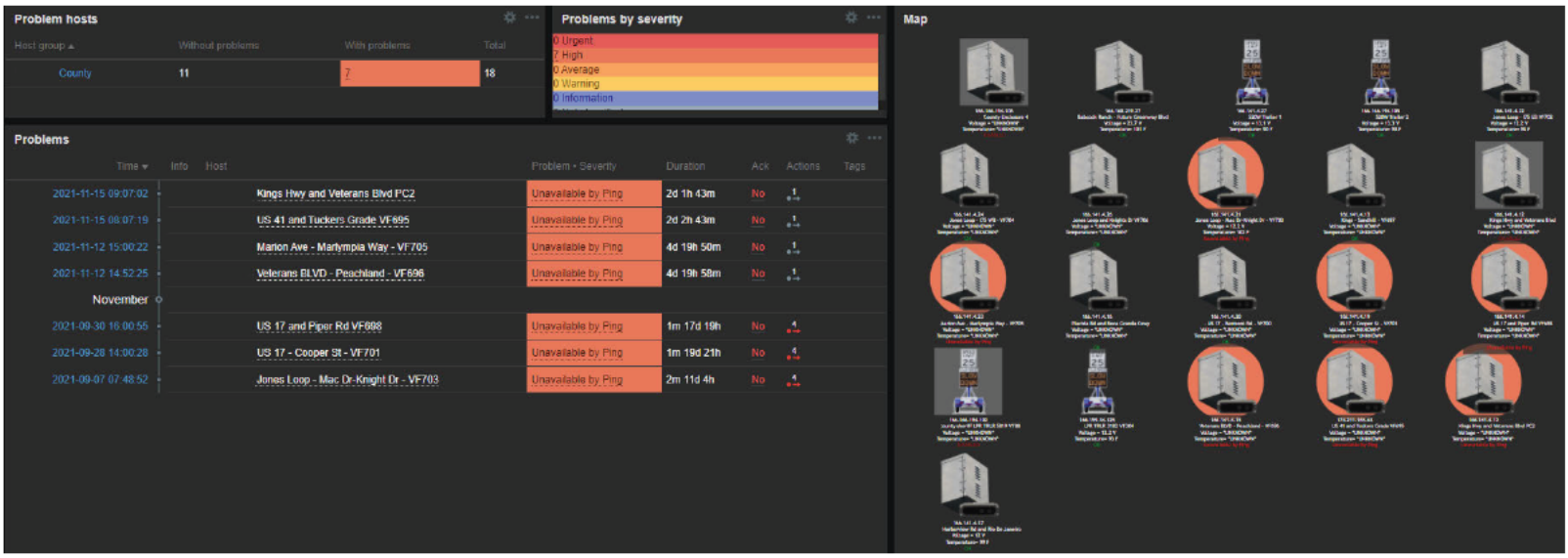
sales@vettedsecuritysolutions.com

vettedsecuritysolutions.com

VETTED VIRTUAL TECHNICIAN

Vetted Virtual Technician is an online tool that monitors the health of all of your field hardware devices in a single, simple-to-use interface. This includes license plate readers, CCTV cameras, wireless radios, trackers, and a host of other devices that allow for an automated triaged support response and rebooting. The system can run self-corrective steps to automatically resolve common issues that would normally require a field visit. VVT can also be customized to monitor unusual and non-standard devices. Alert emails and text messages can be sent to multiple agency administrators when a problem or specific trigger event occurs.





vettedsecuritysolutions.com
4185 35th St N, St. Petersburg, FL 33714

Gabriel, Stephen (POL)

From: Procopio, David (POL)
Sent: Friday, September 25, 2020 10:02 AM
To: Gabriel, Stephen (POL)
Cc: Procopio, David (POL)
Subject: Mid-Shift Notification Criteria

Steve,

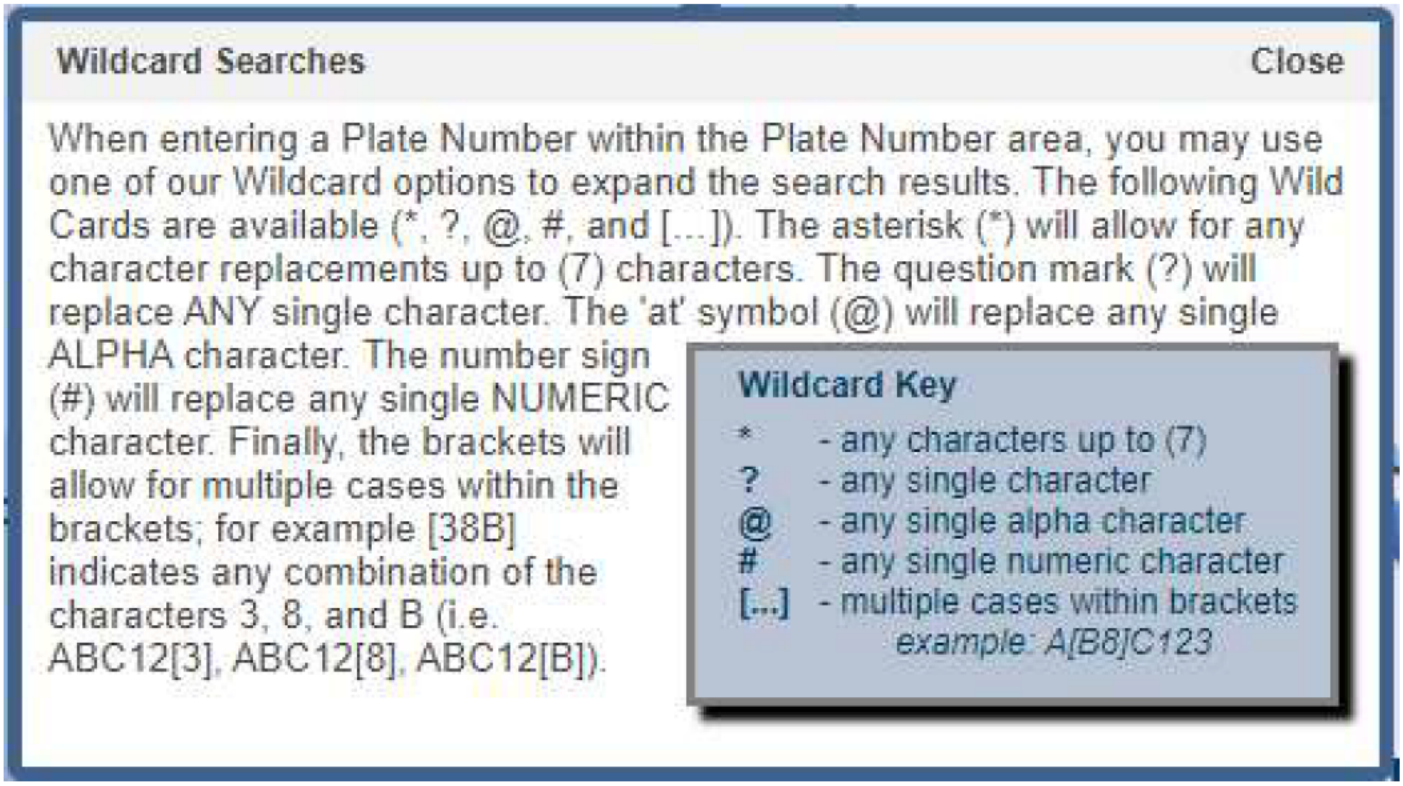
These are the criteria in which the duty offices were instructed to notify me on the mid-shift. This has not been reiterated to the Troop Majors in this current administration; as such I am going to request authorization from LTC Ball to resend at To-From containing these since there are many new duty lieutenants since the last time this was sent.

In the case of extraordinary incidents occurring on the Mid-shift, the Duty Office is asked to please notify Office of Media Relations Director Dave Procopio, either directly or through MSP Operations, of the following specified types of significant incidents that may be expected to generate media interest or present a public safety concern warranting public notification.

- A mass casualty incident;
- An active shooter incident;
- A homicide, shooting, or sexual assault for which MSP is the primary responding agency, for example, a shooting from a vehicle on a highway, or a sexual assault in a state park.
- A police-involved shooting involving a department member;
- Serious or fatal injury to a department member;
- Any incident causing major personal injury or major property damage, for example, an explosion; an aircraft crash; or a catastrophic infrastructure failure such as the Lawrence gas leaks;
- A serious motor vehicle crash involving mass casualties, involving the fatality of a child or children;
- A pending AMBER Alert;
- A missing child or person believed to be in imminent danger for whom investigators want to release descriptive information to the public immediately to assist in the search;
- A State Police pursuit that results in injuries to a department member or member of the public;
- A wanted suspect about whom we want to release information to the public, either in the interest of developing information about the suspect's location or in the interest of public safety;
- Any other significant incident for which the Troop commander requests notification to Media Relations.

In such instances, the Media Relations director will determine whether immediate action is needed, and, if so, whether to handle the incident himself or call out a member of the Media Relations section.

Dave Procopio
Director, Media Communications
Massachusetts State Police



QUICK SEARCH
Wildcard Searches

Standard California Plate format 1ABC234

Plate	WC	Use
A_ _ _ _ _ _	*	A*
1_BC123	@	1@BC123
1ABC_34	#	1ABC#34
1QOQ123	[]	1[QO][QO][QO]123
CUST_M	?	CUST?M

CJIS 2021-2024 Audit Guide

CJIS DOCUMENTATION

1. **CJIS User Agreement**
   - The CJIS 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 CJIS as it relates to the operation, maintenance and security of the systems and services provided.

2. **Global Justice and Public Safety User Agreement**
   - The Global Justice and Public Safety User 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).
   - Applications covered under the Global Justice and Public Safety User Agreement: *Automated License Plate Readers (ALPR), CopLink, EOPSS Data Cross Tracking System, EOPSS National Incident Based Reporting System (NIBRS), My License Office (MLO) and Victim Notification Registry (VNR)*

3. **Memorandum of Understanding- *Police, University, Housing Authority***
   - A memorandum of understanding is required to define the terms, conditions, and mutual responsibilities of each agency 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.

4. **Memorandum of Understanding – *Fire***
   - A memorandum of understanding is required to define the terms, conditions, and mutual responsibilities of each agency 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)

5. **Memorandum of Understanding – *Regional Dispatch***
   - A memorandum of understanding is required to define the terms, conditions, and mutual responsibilities of each agency 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.

6. **Management Control Agreement – *Local IT and/or Vendor IT***
   - The management control agreement covers the overall supervision of all local agency systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of any system that accesses criminal justice information. This agreement must be executed with your agency IT and/or your vendor IT.

7. **FBI Security Addendum – *Vendors, contractors***

- The FBI Security Addendum ensures that adequate security is provided for criminal justice systems while under the control or management of a private entity or connectivity to FBI CJIS systems has been provided to a private entity (contractor/vendor)

8. **Vendor Non-Disclosure Agreement**
   - All vendors are required to complete a non-disclosure agreement stating that s/he has been advised that any disclosure of CORI except as permitted under the sections of law and regulations cited above can result in a fine of up to five thousand dollars ($5,000.00) and/or one year imprisonment in jail or house of correction, in addition to civil liability for damages pursuant to § 177 including exemplary damages, and a civil fine of up to five hundred dollars ($500.00) per violation if the DCJIS finds such a willful violation.

9. **Individual Non-Disclosure Agreement**
   - While not required, CJIS highly recommends that each agency have every member of staff sign an Individual Non-Disclosure Agreement and keep on file at your agency.

CJIS POLICIES

10. **CJIS Comprehensive Policy**

The CJIS comprehensive policy is a collection of policies that each department is required to have within their departmental policies to address regulations, procedures, and requirements as outlined in the FBI Security Policy as well as Code of Massachusetts Regulations 803.

The following policies are individual policies listed within the comprehensive policy that address the following subject areas. These policies should be included in your departmental policies:

10A. Acceptable Use Policy
- All agencies must have policies and procedures for the acceptable use of all CORI and criminal justice information

10B. Misuse Policy
- All agencies must outline the penalties for the improper access, dissemination, and handling of CJIS data

10C. Media Disposal Policy
- All agencies must have proper procedures in place the proper disposal of all media and criminal justice information

10D. Physical Security Policy
- All agencies must have proper procedures in place for the physical protection and security control of all criminal justice information.

10E. Computer Security Incident Report Policy
- All computer security incidents must be reported with 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.

10F. Secondary Dissemination
- All agencies must maintain central secondary dissemination log to record any dissemination of CORI outside this organization, including dissemination at the request of the subject.

10G. Employee Fingerprinting Policy
- The CJIS User Agreement and the FBI CJIS Security Policy require each CJIS agency to conduct fingerprint-based criminal record checks on all personnel

prior to hire and at least once every five years thereafter.
- In addition, agencies must conduct fingerprint-based criminal record checks on all other individuals who have unescorted access to secure (non-public) areas of the agency prior to allowing access. These individuals include IT personnel, contractors, vendors, custodians, and volunteers.

10H. Civil Fingerprinting Policy
- The purpose of this document is to establish uniform policies and procedures for the collection and submission of civil fingerprints by municipalities to screen applicants for certain municipal licenses and for the collection of fees associated with this process

10I. Automated License Plate Reader Policy (if applicable)
- All agencies, if applicable, must have policies and procedures for the acceptable use of Automated License Plate Readers

INFORMATION TECHNOLOGY

11. Maintenance Agreement
- The maintenance agreement is the proof of purchase of services by a CJIS certified vendor to maintain and provide support for your CJIS router located within your agency. To meet this requirement, the agency is required to provide a current invoice with Integration Partners or any CJIS certified vendor indicating that these services have been procured by the agency.

12. CJIS Network Diagram
- The CJIS Network Diagram is a diagram that documents how your agency's information technology equipment is connected to the CJIS router and switch.

13. System Use Notification Screen ("Splash Screen")
- The system use notification screen is a warning screen that is commonly referred to as a "splash screen." The splash screen should appear before a user can log into their computer. The following language should be at minimum in the system use notification:

  "This system is owned by _____ and contains confidential information. Access to this system is restricted to authorized users for the purposes of fulfilling their duties of employment. Use of this system may be monitored and is subjected to all applicable laws, regulations, and _____ policies and procedures.

14. Advanced Authentication
- Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password on mobile devices. Examples include but are not limited to such as: biometric systems, public key infrastructure (PKI)), authenticator is sent on demand via text message, phone call, etc.), or high-risk challenge/response questions.

15. FIPS-2 Encryption certificate
- When CJI is transmitted or accessed from outside a physically secure location, it is required that the cryptographic module is FIPS 140-2 certified and uses a symmetric cipher key strength of at least 128-bit strength to protect Criminal Justice Information (CJI). All agencies should be prepared to provide FIPS 140-2 certificates associated with all access and transmission of CJI outside the physically secure locations.

16. Strong Password Policy
- In keeping with the FBI CJIS Security Policy and industry best practices, access to any CJIS application requires the use of a strong password. These requirements will ensure the security and integrity of all CJIS and FBI systems and the information they contain.

17. **Event Logging**
    - Event logging is required on the local domain level to ensure that if a security-related event occurred in relation to FBI/CJI, your agency could identify who did it, where (what information systems), and when it happened. CJIS is responsible for the collection of this information for applications CJIS manages. Local agencies do not need to include CJIS managed information systems/applications in the event log. If the agency is using CJIS Single Sign-On through Windows Active Directory, some logs may already be maintained at the domain level.

CJIS REPRESENTATIVE RESPONSIBILITIES

18. **Agency Head CJIS Responsibilities**
    - All Agency Heads are responsible for ensuring compliance with FBI and CJIS rules, regulations, and procedures. It is recommended that your agency codify within your departmental policies the responsibilities of an agency head as prescribed in the CJIS User Agreement

19. **CJIS Representative Responsibilities**
    - All CJIS Representatives are responsible for ensuring compliance with FBI and CJIS rules, regulations, and procedures. It is recommended that your agency codify within your departmental policies the responsibilities of a CJIS Representative as prescribed in the CJIS User Agreement

20. **User Account Validation Policy**
    - All internal network accounts and RMS user accounts shall be reviewed at least every six months by the terminal agency coordinator (TAC) or his/her designee to ensure that access and account privileges commensurate with job functions, need-to- know, and employment status on systems that contain Criminal Justice Information.

21. **NexTest - Security Awareness Training**
    - All authorized CJIS users must complete NexTest Security Awareness training before being granted CJIS user account credentials, and every two (2) years thereafter. At the time of your audit, your agency's NexTest expiration report should indicate that all authorized users are up to date with their security awareness training to be in compliance.

22. **CJISOnline.com –Security Awareness Training**
    - Any unescorted staff that do not have CJIS users accounts and are not authorized to use CJIS, but have access to secured areas, must take Security Awareness Training at CJISonline.com
        - **Security and Privacy Basic Role (formerly Level 1)**
            - Administrative staff, custodial services, maintenance, vendors, etc.
        - **Security and Privacy Privileged Role (formerly Level 4)**
            - Information Technology personnel including system administrators, security administrators, network administrator, vendors, etc.
        - **Security and Privacy Security Role (formerly LASO Certification)**
            - Each agency must have a user designated as the Local Agency Security Officer who must complete this training.

23. **XML/CAD roster**

- All agencies who run queries through their records management system (RMS/CAD) must provide CJIS with an XML/CAD roster with the unique identifier/username for each user within your agency

DATA QUALITY REVIEW

24. Data Quality Review

- During your CJIS Audit, an on-site data quality review is conducted. Your auditor will compare NCIC (OpenFox) records against agency case files and original documents to determine the validity, accuracy, completeness, and timely entry/removal of records are verified. A list of records to pull for review will be forwarded to you before your audit.

FELONY ARRAIGNMENT REVIEW

25. Felony Arraignment Review

- Pursuant to M.G.L. c. 263, § 1A and 803 CMR 7.08, 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. Your agency will be provided with a list of felony arraignments that will need to be reviewed.

The Commonwealth of Massachusetts
Department of State Police

MAURA T. HEALEY
GOVERNOR

KIMBERLEY DRISCOLL
LIEUTENANT GOVERNOR

TERRENCE M. REIDY
SECRETARY

JOHN E. MAWN JR.
COLONEL/SUPERINTENDENT

JOHN D. PINKHAM
DEPUTY SUPERINTENDENT

August 24, 2023

TO: Judith Williford, Program Manager, US Department of Justice, Office of Community Oriented Policing Services
FROM: Melissa Comeau, Director of Billing, Receivables and Grants, Massachusetts State Police

RE: COPS Anti-Heroin Task Force 2020 – Grant Adjustment Modification, Award # 2020HPWX0004

Dear Program Manager Williford,

The Massachusetts State Police (MSP) respectfully requests a grant budget modification transferring $439,250 from the Contracts and Consultants category and transferring $125,750 from the Other Costs category and moving $564,000 to the Equipment and Technology category and moving $1,000 to the Supplies category.

The MSP's Anti-Heroin Task Force strategy focuses on disrupting and dismantling Drug Trafficking Organizations. Critically important to this mission is the ability to apprehend offenders who traffic and distribute heroin/fentanyl and to seize the heroin and fentanyl in their possession, preventing it from circulating in our communities. High-level narcotics offenders routinely flee from police when attempts are made to stop and apprehend them. The StarChase GPS vehicle mounted launcher (VML) is pursuit mitigation technology, which allows law enforcement to deploy a temporary GPS tracking device onto a target vehicle during an attempted arrest. This allows investigators to monitor the movement of the target vehicle in real time while backing off the pursuit. This technology would allow MSP to apprehend high-level narcotics offenders while simultaneously reducing risks to the public, police, and the suspects and would increase the successful seizure of narcotics, firearms, and evidence. The MSP requests to purchase (30) StarChase VML devices and two portable devices at a total cost of $340,000. StarChase devices would be strategically deployed to support MSP drug units and uniformed Troopers that are involved in arrests of high-level narcotics offenders and the vehicle pursuits that often follow.

The MSP operates an Automatic License Plate Recognition (ALPR) camera system that allows MSP to get near real-time alerts (hits) on the locations of suspected drug traffickers. It provides historical search capability for identified drug trafficking vehicles for patterns of activity. The Massachusetts State Police manages the ALPR system and allows local and federal law enforcement to access data from the system, thus solidifying partnerships and promoting the open exchange of information among agencies. The MSP wishes to purchase ALPR equipment at a total cost of $110,000 to replace current aging equipment.

The MSP's Technical Services Unit (TSU) assists Federal, State, and Local police by providing technical support and technology-based tools to aid in heroin and fentanyl investigations. The MSP requests to purchase Oculus covert surveillance equipment that will be used to collect audio and video evidence for investigations directly related to heroin and fentanyl distribution and trafficking. In addition, The MSP also requests to purchase G3 Technologies NOMOS WIFI Spectrum Clearing Tools for officer safety purposes during investigations directly related to heroin/fentanyl distribution and trafficking. The TSU has recently received multiple requests to provide such support and have been unable to assist. These tools will allow investigators to

safely gather critical evidence to further enhance heroin/fentanyl investigations and contribute greatly to successful prosecutions.

The MSP's Technical Services Unit (TSU) is responsible for management of video evidence related to narcotics investigations with a focus on heroin and fentanyl distribution and trafficking. The TSU is in need of external hard drives for storage of video evidence. The MSP requests to purchase (12) – 8TB, (16) – 6TB and (25) – 4TB external drives in the supplies category.

Acquisition of the above updated technology will greatly enhance MSP's anti-heroin and other opioid long-term strategy and goals by providing a user-friendly and effective tool to assist with investigative leads, identify potential drug shipment alerts as well as track DTO's.

Proposed modifications are as follows:

A. SWORN OFFICERS - No changes requested

B. CIVILIAN AND NON-SWORN PERSONNEL - No changes requested

C. EQUIPMENT AND TECHNOLOGY

- Increase category by $564,000 for pursuit mitigation equipment, ALPR and surveillance equipment.

D. SUPPLIES

- Increase category by $1,000 for external hard drives

E. TRAVEL/TRAINING

- No changes requested

F. CONTRACTS AND CONSULTANTS

- Decrease category by $439,250

G. OTHER

- Decrease Other Costs category by $125,750

FFY2020 COPS Office Anti-Heroin Task Force Program (AHTF)
7/1/2020 - 6/30/2024
MMARS Appropr: 8100-3000 Progr: F20HPWX004

Budget Category	Approved Budget	Budget Changes with GAM GAM 570765 - Approved	Budget Changes with GAM GAM 574447 - Approved	Current Revised Budget	August 2023 Pending Budget Modification	Pending Revised Budget
Sworn Officers	**$0.00**	**$0.00**	**$0.00**	**$0.00**		$0.00
Civilian and Non-Sworn Personnel	**$0.00**	**$0.00**	**$0.00**	**$0.00**		$0.00
Equipment and Technology	**$52,615.80**	**$329,915.92**	**$0.00**	**$592,531.72**	$564,000.00	**$1,156,531.72**
Supplies	**$83,915.65**	**$2,327.71**	**$0.00**	**$86,243.36**	$1,000.00	**$87,243.36**
Travel, Training	**$0.00**	**$0.00**	**$0.00**	**$0.00**		**$0.00**
Contracts and Consultants	**$1,620,000.00**	**-$332,243.63**	**$0.00**	**$727,756.87**	-$439,250.00	**$288,506.87**
Other	**$2,232,243.05**	**$0.00**	**$0.00**	**$2,582,243.05**	-$125,750.00	**$2,456,493.05**
PLX Software	$35,468.25	$0.00	$0.00	$35,468.25	-$35,468.25	$0.00
PLX License Support (36 mos)	$18,720.00	$0.00	$0.00	$18,720.00	-$18,720.00	$0.00
Clearview Software (36 mos)	$18,000.00	$0.00	$0.00	$18,000.00	-$18,000.00	$0.00
Microsoft Office (70)	$23,432.50	$0.00	$0.00	$23,432.50	-$23,432.50	$0.00
Windows Enterprise Upgrade & Software (70)	$18,890.20	$0.00	$0.00	$18,890.20	-$18,890.20	$0.00
Wire Costs (3 lines x 3 task forces x 3 months) T-Mobile	$114,750.00	$0.00	$0.00	$114,750.00	-$11,239.05	$103,510.95
Overtime for Task For Officers -	$533,300.00	$0.00	-$19,001.20	$864,298.80	$0.00	$864,298.80
Overtime for Addl Officers Investigative Support (Local	$319,682.10	$0.00	$0.00	$319,682.10	$0.00	$319,682.10
Overtime for Troopers Assigned to Task Forces	$1,150,000.00	$0.00	$0.00	$1,150,000.00	$0.00	$1,150,000.00
Payroll Tax @ 1.85%			$19,001.20	$19,001.20	$0.00	$19,001.20
TOTAL Budget	**$3,988,775.00**	**$0.00**	**$0.00**	**$3,988,775.00**	**$0.00**	**$3,988,775.00**

Thank you for your attention to this matter. If you have questions or need additional information regarding this budget modification, please contact me at 508-820-2137.

Sincerely,

Melissa Comeau

Director of Billing, Receivables & Grants

(508) 820-2137

The Commonwealth of Massachusetts
Department of State Police

MAURA T. HEALEY
GOVERNOR

KIMBERLEY DRISCOLL
LIEUTENANT GOVERNOR

TERRENCE M. REIDY
SECRETARY

JOHN E. MAWN JR.
COLONEL/SUPERINTENDENT

JOHN D. PINKHAM
DEPUTY SUPERINTENDENT

October 17, 2023

TO: Judith Williford, Program Manager, US Department of Justice, Office of Community Oriented Policing Services
FROM: Melissa Comeau, Director of Billing, Receivables and Grants, Massachusetts State Police

RE: COPS Anti-Heroin Task Force 2020 – Grant Adjustment Modification, Award # 2020HPWX0004

Dear Program Manager Williford,

The Massachusetts State Police (MSP) respectfully requests a grant budget modification transferring $425,500 from the Contracts and Consultants category and $164,000 from the Other Costs category. We would like to reallocate to the following categories: $584,000 to Equipment and Technology and $5,500 to Supplies.

The MSP's Anti-Heroin Task Force strategy focuses on disrupting and dismantling Drug Trafficking Organizations. Critically important to this mission is the ability to apprehend offenders who traffic and distribute heroin/fentanyl and to seize the heroin and fentanyl in their possession, preventing it from circulating in our communities. High-level narcotics offenders routinely flee from police when attempts are made to stop and apprehend them. The StarChase GPS vehicle mounted launcher (VML) is pursuit mitigation technology, which allows law enforcement to deploy a temporary GPS tracking device onto a target vehicle during an attempted arrest. This allows investigators to monitor the movement of the target vehicle in real time while backing off the pursuit. This technology would allow MSP to apprehend high-level narcotics offenders while simultaneously reducing risks to the public, police, and the suspects and would increase the successful seizure of narcotics, firearms, and evidence. The MSP requests to purchase (30) StarChase VML devices and two portable devices at a total cost of $340,000. StarChase devices would be strategically deployed to support MSP drug units and uniformed Troopers that are involved in arrests of high-level narcotics offenders and the vehicle pursuits that often follow.

The MSP operates an Automatic License Plate Recognition (ALPR) camera system that allows MSP to get near real-time alerts (hits) on the locations of suspected drug traffickers. It provides historical search capability for identified drug trafficking vehicles for patterns of activity. The Massachusetts State Police manages the ALPR system and allows local and federal law enforcement to access data from the system, thus solidifying partnerships and promoting the open exchange of information among agencies. The MSP wishes to purchase ALPR equipment at a total cost of $125,000 to replace current aging equipment.

The MSP's Technical Services Unit (TSU) assists Federal, State, and Local police by providing technical support and technology-based tools to aid in heroin and fentanyl investigations. The MSP requests to purchase Oculus covert surveillance equipment that will be used to collect audio and video evidence for investigations directly related to heroin and fentanyl distribution and trafficking.

In addition, The MSP also requests to purchase G3 Technologies NOMOS WIFI Spectrum Clearing Tools for officer safety purposes during investigations directly related to heroin/fentanyl distribution and trafficking. The TSU has recently received multiple requests to provide such support and have been unable to assist. These tools will allow investigators to safely gather critical evidence to further enhance heroin/fentanyl investigations and contribute greatly to successful prosecutions.

The MSP's Technical Services Unit (TSU) is responsible for management of video evidence related to narcotics investigations with a focus on heroin and fentanyl distribution and trafficking. The TSU is in need of external hard drives for storage of video evidence. The MSP requests to purchase (12) – 8TB, (16) – 6TB and (25) – 4TB external drives in the Supplies category.

The MSP's CINRET requests to purchase two GPS Tracking devices that are used under a court order to track target vehicles during narcotic investigations. The MSP's CINRET also requests to purchase four digital cameras to assist with their fentanyl and heroin investigation. They are needed to facilitate the proper documentation of evidence and surveillance photos of targets and locations.

The MSP's CLET requests to purchase a digital scale for weighing the seized precursor chemicals.

Acquisition of the above updated technology will greatly enhance MSP's anti-heroin and other opioid long-term strategy and goals by providing a user-friendly and effective tool to assist with investigative leads, identify potential drug shipment alerts as well as track DTO's.

Proposed modifications are as follows:

A. SWORN OFFICERS - No changes requested

B. CIVILIAN AND NON-SWORN PERSONNEL - No changes requested

C. EQUIPMENT AND TECHNOLOGY

- Increase category by $584,000 for pursuit mitigation equipment, ALPR and surveillance equipment.

D. SUPPLIES

- Increase category by $5,500 for external hard drives, digital cameras and digital scale

E. TRAVEL/TRAINING

- No changes requested

F. CONTRACTS AND CONSULTANTS

- Decrease category by $425,500

G. OTHER

- Decrease Other Costs category by $164,000

	FFY2020 COPS Office Anti-Heroin Task Force Program (AHTF) 7/1/2020 - 6/30/2024 MMARS Appropr: 8100-3000 Progr: F20HPWX004					October 2023	
		Approved Budget	Budget Changes with GAM GAM 570765 - Approved	Budget Changes with GAM GAM 574447 - Approved	Current Revised Budget	Pending Budget Modification	Pending Revised Budget
	Budget Category						
A	**Sworn Officers**	**$0.00**	**$0.00**	**$0.00**	**$0.00**		$0.00
B	**Civilian and Non-Sworn Personnel**	**$0.00**	**$0.00**	**$0.00**	**$0.00**		$0.00
C	**Equipment and Technology**	**$52,615.80**	**$329,915.92**	**$0.00**	**$592,531.72**	$584,000.00	**$1,176,531.72**
D	**Supplies**	**$83,915.65**	**$2,327.71**	**$0.00**	**$86,243.36**	$5,500.00	**$91,743.36**
E	**Travel, Training**	**$0.00**	**$0.00**	**$0.00**	**$0.00**		**$0.00**
F	**Contracts and Consultants**	**$1,620,000.00**	**-$332,243.63**	**$0.00**	**$727,756.87**	-$425,500.00	**$302,256.87**
G	**Other**	**$2,232,243.05**	**$0.00**	**$0.00**	**$2,582,243.05**	-$164,000.00	**$2,418,243.05**
	PLX Software	$35,468.25	$0.00	$0.00	$35,468.25	-$35,468.25	$0.00
	PLX License Support (36 mos)	$18,720.00	$0.00	$0.00	$18,720.00	-$18,720.00	$0.00
	Clearview Software (36 mos)	$18,000.00	$0.00	$0.00	$18,000.00	-$18,000.00	$0.00
	Microsoft Office (70)	$23,432.50	$0.00	$0.00	$23,432.50	$0.00	$23,432.50
	Windows Enterprise Upgrade & Software (70)	$18,890.20	$0.00	$0.00	$18,890.20	$0.00	$18,890.20
	Wire Costs (3 lines x 3 task forces x 3 months) T-Mobile	$114,750.00	$0.00	$0.00	$114,750.00	-$87,811.75	$26,938.25
	Overtime for Task For Officers -	$533,300.00	$0.00	-$19,001.20	$864,298.80	-$4,000.00	$860,298.80
	Overtime for Addl Officers Investigative Support (Local	$319,682.10	$0.00	$0.00	$319,682.10	$0.00	$319,682.10
	Overtime for Troopers Assigned to Task Forces	$1,150,000.00	$0.00	$0.00	$1,150,000.00	$0.00	$1,150,000.00
	Payroll Tax @ 1.85%			$19,001.20	$19,001.20	$0.00	$19,001.20
	TOTAL Budget	**$3,988,775.00**	**$0.00**	**$0.00**	**$3,988,775.00**	**$0.00**	**$3,988,775.00**

Thank you for your attention to this matter. If you have questions or need additional information regarding this budget modification, please contact me at 508-820-2137.

Sincerely,

Melissa Comeau

Director of Billing, Receivables & Grants

(508) 820-2137

Division of Homeland Security and Preparedness
Annual Report 2022

Commonwealth Fusion Center

Mission

The Commonwealth Fusion Center (CFC) collects and analyzes information to produce and disseminate actionable intelligence to stakeholders for strategic and tactical decision-making. This is done to identify, disrupt, or deter criminal activity and terrorism, both domestic and international.

Overview

The CFC, established in 2004, is an all-crimes fusion center that serves as the Commonwealth's Principal Center for Information Collection and Dissemination pursuant to Executive Order No. 476. The CFC works in collaboration with local, state, and federal agencies and the private sector to improve public safety and enhance homeland security throughout the Commonwealth, New England, and the Nation. Furthermore, it is the Commonwealth's central repository for homeland security information, criminal intelligence, and critical incident reporting.

The CFC emphasizes threat detection and reporting, creating new best practices, enhanced special event support, outreach efforts, and collaboration. The CFC also plays a lead role during critical incidents, special events, and important public safety initiatives.
The Commonwealth Fusion Center Program is comprised of four units, each working in cooperation with the others:

Anti-Terrorism Unit (ATU) –This unit performs investigatory functions, and its members serve on a Federal Bureau of Investigation Joint Terrorism Task Force.

Criminal Information Section (CIS) – This section is responsible for activities associated with protecting critical infrastructure, cybersecurity, and drug enforcement.

Intelligence Services Unit (ISU) – The ISU is comprised of civilian analysts and support staff who perform Watch Center functions, intelligence analysis, case support, special event support, and suspicious activity vetting.

Watch Center Unit (Watch) – The Watch operates 24/7. It performs situational awareness functions and provides tactical intelligence during critical incidents.

Programs

Massachusetts Cybersecurity Program (MCP)- The MCP program focuses on cybersecurity threat reporting, training, education, and awareness. As a part of its activities, the MCP routinely distributes cybersecurity intelligence products, situational awareness messages, and a monthly open-source bulletin to its members. During 2022, the MCP created and disseminated 16 Cybersecurity awareness products and 12 monthly cybersecurity bulletins and re-disseminated 136 cyber intelligence products and alerts on behalf of other agencies to over 697 local, state, federal, and private sector members. Additionally, MCP members provided 54 cybersecurity briefings.

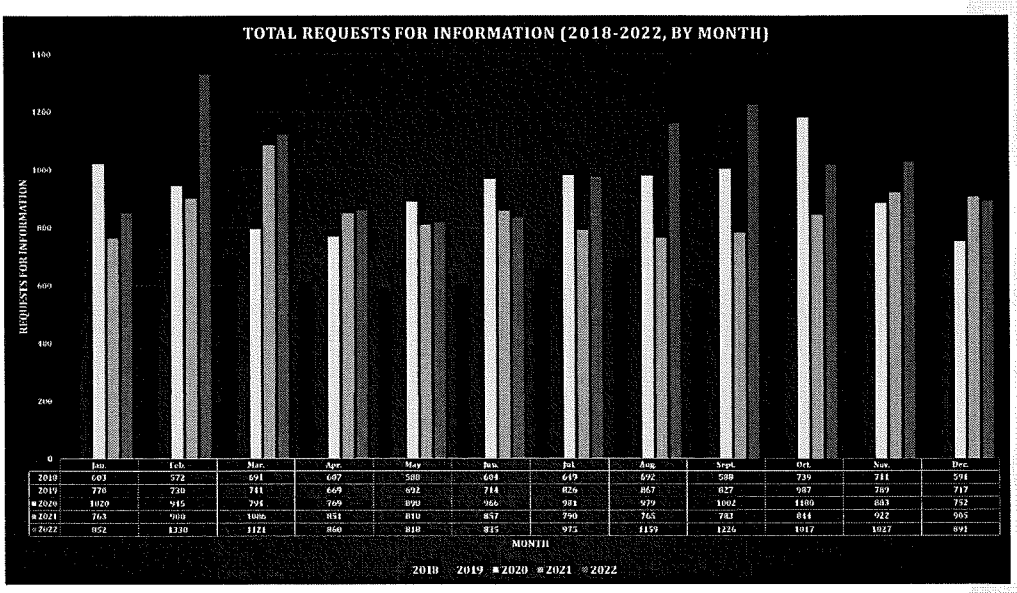
The MCP Vulnerability and Threat Intelligence Project was established in March 2020 to identify municipalities and critical infrastructure sector partners within the Commonwealth with critical cyber vulnerabilities that pose an immediate threat of exploitation by threat actors, including ransomware and data breaches. Once these cyber vulnerabilities are identified, the Massachusetts Cybersecurity Program notifies the affected organizations and over one hundred notifications have been made since the program's inception. In addition, 13 cyber incidents were reported to the MCP in 2022.

Commonwealth Critical Infrastructure Program (CCIP)- The CFC runs the CCIP, created in 2005 to implement a statewide, coordinated approach to identifying and protecting the Commonwealth's critical infrastructure and key resources. The CCIP disseminated 16 CCIP bulletins and 109 critical infrastructure-related products on behalf of other agencies in 2022.

Requests for Information (RFI)

During 2022, the CFC received & responded to 13,487 RFIs from local, state, and federal law enforcement agencies. This was a 31% increase over the previous year. A single RFI may require the performance of multiple database checks, the submission or response to an HSIN Exchange Request, the creation of a GIS map or other product, a response to a Terrorist Screening Center (TSC) hit, or a response to a request for technical support. In 2022, of the 13,487 Requests for Information received: 12,111 (89%) were for CFC database checks.

- State/Local Agencies: 11,212
- Federal Agencies: 538
- Other Fusion Centers: 290
- Other/Unclassified: 71



	Jan.	Feb.	Mar.	Apr.	May	Jun.	Jul.	Aug.	Sept.	Oct.	Nov.	Dec.
2018	603	572	691	607	580	604	649	692	598	739	711	591
2019	776	730	741	669	692	714	826	867	827	987	769	717
2020	1020	945	795	769	890	966	984	979	1002	1180	883	752
2021	763	900	1086	854	810	857	790	765	783	844	922	905
2022	852	1330	1121	860	818	815	973	1159	1226	1017	1027	891

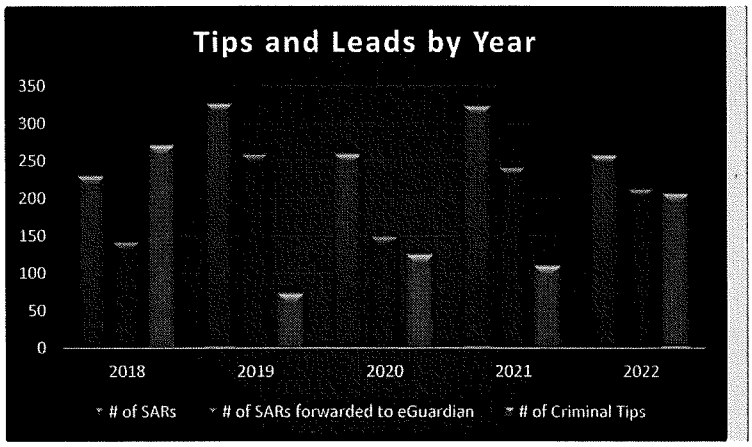
INTERPOL

The CFC is the state liaison coordinator for Interpol in Massachusetts. The CFC Interpol liaison coordinates with Interpol Washington to support members of the international law enforcement community. In 2022, the CFC received and responded to 31 Interpol requests for information or assistance from 20 countries, including the United Kingdom, Ireland, Jamaica, Romania, France, the Netherlands, Switzerland, and Canada.

The CFC has assisted Interpol partner agencies with investigations ranging from fraud, human trafficking, threats to life, and homicide, as well as identifying, locating, and facilitating well-being checks on suicidal and missing persons.

Suspicious Activity Reporting (SARs) and Criminal Tips

During 2022, the Commonwealth Fusion Center processed 209 criminal tips with no potential nexus to terrorism and 260 Suspicious Activity Reports (SARs) with a potential nexus to terrorism. Of the 260 SARs with a potential nexus to terrorism, 215 were forwarded to eGuardian.



Situational Awareness and Intelligence Products

In 2022, the CFC produced four quarterly threat assessments focused on pertinent intelligence that could impact the Commonwealth of Massachusetts. In addition, the CFC produced numerous situational awareness messages related to terrorist attacks, violent criminal incidents, mass casualty attacks, civil unrest, products related to physical threats, and cybersecurity threats to critical infrastructure. The CFC created new, innovative product lines in 2022, including the weekly *Massachusetts Tactical Research & Intelligence Exchange (Matrix)* and two new quarterly products, including the *MSP Quarterly Crime Gun Review* and a joint CFC and NEHIDTA *Massachusetts Drug Trafficking Trends - Quarterly Intelligence Bulletin.*

In 2022, the CFC disseminated **1,955** Situational Awareness Bulletins, Intelligence Products, and other advisories to local, state, and federal law enforcement agencies.

Training and Seminars

In 2022, CFC personnel provided in-person and virtual training to local, state, and federal law enforcement partners. Training on CFC Resources, Coplink, Privacy/Civil Rights and Civil Liberties (P/CRCL), the Current Threat Environment, and Threat Reporting was provided to **793** individuals.

The CFC also held three specialized seminars.

- **School Safety and Security Seminar**
  The CFC's 5th Annual School Safety and Security Seminar was held in December 2022. There were more than **130** attendees at this year's event. The seminar included the following topics of discussion: Massachusetts Cybersecurity Program Overview, Common Cyber Attacks / Threats, Electronic Evidence Considerations, Cyber Hygiene & Best Practices, and Reporting to Law Enforcement.

- **Faith-Based Safety and Security Seminar**
  The CFC held its 4th Annual Faith Based Safety and Security Seminar in November 2022. There were **120** faith-based partners in attendance including local, state, and federal government members. The seminar focused on the physical threat environment, including the targeting of faith-based organizations, and the cyber threat environment, including the targeting of faith-based organizations, suspicious activity reporting protocols, and grants opportunities.

- **Private Sector Safety and Security Seminar**
  The CFC held its 3rd Annual Private Sector Safety and Security Seminar focused on cybersecurity and physical security in November 2022 for more than **60** private sector attendees. Topics of discussion included a critical infrastructure threat overview, a cybersecurity threat overview, and threat reporting protocols.

Boston Marathon

The CFC provided intelligence and special event support for the 126th Boston Marathon, which was held on April 18, 2022. Special event support included: Commanding the Intelligence/Investigations Working Group; Overseeing the development of a Joint Special Event Assessment; Providing intelligence briefings for key stakeholders and decision-makers throughout the special event planning process as well as during the event itself; Deploying intelligence analysts to command posts to assist with vetting suspicious activity and suspicious individuals.

Success Stories

On March 28, 2022, the CFC observed a post directed to the official MSP Facebook page from a concerned citizen regarding a YouTube video in which a MA registered vehicle is shown with an electronic scrolling sign displaying multiple expressed/implied threats. One of the messages directly threatened U.S. President Joe Biden. A query of the MA registration identified a registered owner/operator that was the subject of a similar Suspicious Activity Report (SAR) in 2020. Members of the MSP Anti-Terrorism Unit (ATU) and U.S. Secret Service (USSS) were advised and investigated the incident.

On July 9, 2022, the CFC was made aware of an individual residing in MA who threatened to travel to San Francisco, CA, and blow-up Reddit Headquarters with a pipe bomb. The suspect allegedly learned how to manufacture explosive devices from the internet and suffered from mental health issues. A BOLO/Officer Safety was created by the CFC and distributed to partner fusion centers. Partner law enforcement agencies in multiple states, including RI, NY, IN, WY, and MN, responded with information and Automated License Plate Recognition data on the suspect's vehicle, allowing investigators to attempt to intercept the vehicle. A full extradition warrant was issued for the suspect. After multiple days of investigation, the suspect was ultimately located in Springfield, MO, and taken into custody without incident.

On August 11, 2022, the CFC was advised of a suspicious phone call made to the Massachusetts Bar Association. The caller stated that he had just killed his brother and needed an attorney.

Using law enforcement and open-source investigative tools, personnel assigned to the CFC tentatively identified the caller and potential victim and contact the local police departments in Easton, Brockton, and Weymouth, where the suspect and victim had associated addresses. While investigators attempted to locate the victim, State Police Operations initiated a 'ping' on the suspect's phone through T-Mobile. They obtained geolocation data for the caller in Hingham, MA. The alleged victim was located and reported that his brother had assaulted him with a firearm and fired shots at his residence. The Hingham Police Department was contacted and coordinated with the Weymouth Police Department to locate and initiate a motor vehicle stop on the suspect's vehicle. The suspect was ultimately taken into custody without incident. Due to effective coordination and collaboration between the Commonwealth Fusion Center, State Police Operations, and local law enforcement partners (Weymouth, Easton, Brockton, Hingham), the total elapsed time from the initial call to the apprehension of the shooter was approximately one (1) hour.

Anti-Terrorism (ATU)

Overview

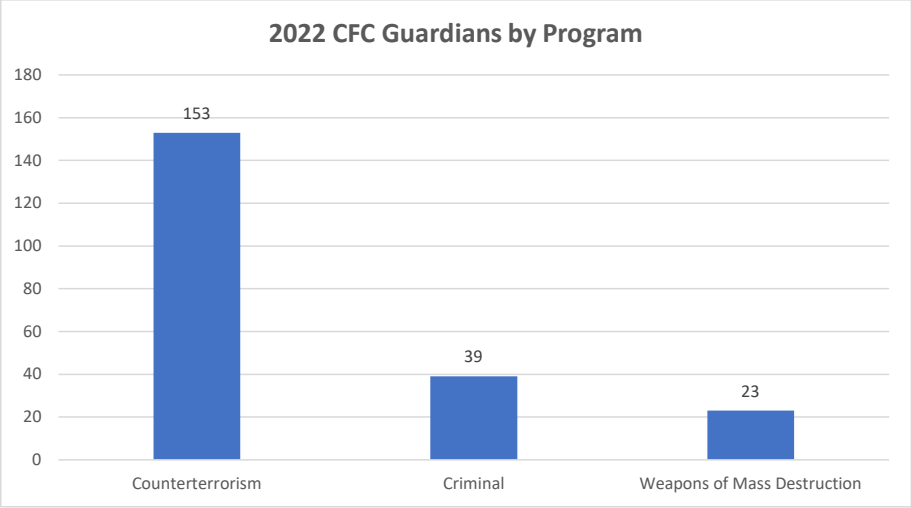
The Anti-Terrorism Unit (ATU) is a state-wide investigative unit under the Massachusetts State Police Division of Homeland Security and Preparedness. State Police ATU members are jointly assigned through a memorandum of agreement (MOU) to the Boston Division of the Federal Bureau of Investigation (FBI) Joint Terrorism Task Force (JTTF). All members are deputized as Special Deputy US Marshalls with authority to investigate US Code Title 28 violations further defined as "The unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."

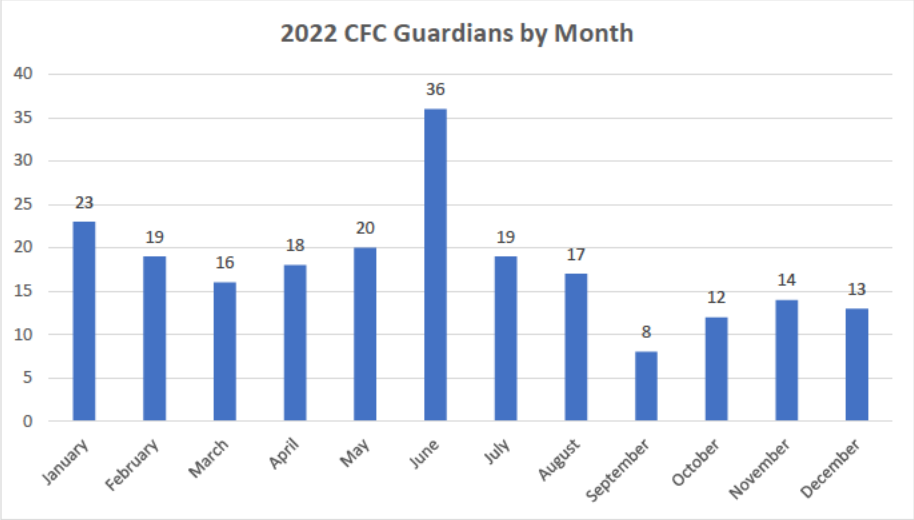
Mission

The Anti-Terrorism Unit's primary mission is to investigate and seek prosecution of individuals who violate federal statutes relating to domestic and international terrorism. These responsibilities include working with the United States Attorney's Office to write unclassified and classified Foreign Intelligence Surveillance Act (FISA) search warrants; conduct Guardian threat assessments; conduct preliminary and full investigations; and provide liaison to the FBI and other federal, state, and local law enforcement agencies relating to homeland security matters. ATU members routinely conduct surveillance, recruit, train, and handle Confidential Human Sources (CHS), collect domestic and international intelligence, and prepare intelligence briefings for special events. Additionally, the ATU provides 24-hour land-based security for Liquid Natural Gas (LNG) deliveries, assists federal partners in search/arrest warrants, and protects dignitaries when traveling through the Commonwealth.

2022 Metrics

- Investigated 338 leads within ACISS
- 260 suspicious activity reports (SARs) were received and vetted in 2022
- 215 of the SARs were forwarded to the JTTF for further action
- Investigated 132 Guardian leads
- Conducted 127 federal and state agency assists
- 10 LNG security/intelligence missions performed
- Conducted intelligence for 2022 protests
  - Conducted intelligence for the Boston Marathon, 4th of July Celebration, LIV Golf Tournament, and New England Patriots games
- ATU members are on-call 24/7/365 for all terrorism matters

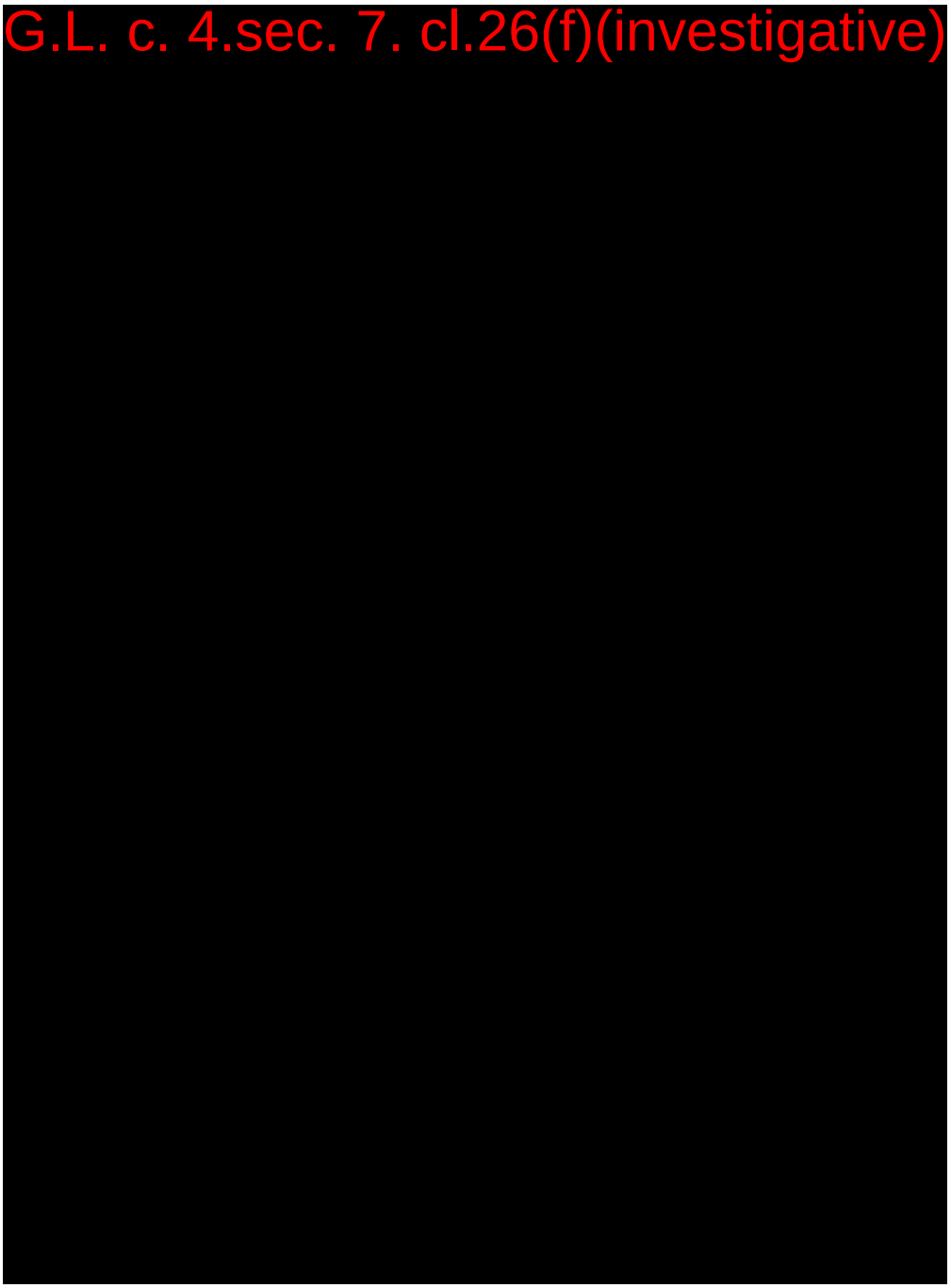




Significant Activities and Investigations

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

[redacted]


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

[redacted]

Behavioral Observation and Suspicious Activity Recognition (BOSAR)

MISSION

The BOSAR Unit, short for Behavioral Observation and Suspicious Activity Recognition, is the Department's key asset for plainclothes, covert observation, and surveillance during large-scale events. Its primary objective is to swiftly detect any "hostile" behavior and mitigate potential harm to the public, essentially to prevent the preventable. BOSAR carries out two distinct missions, namely training and operational, to fulfill its mission effectively.

From 2014 to 2022, the BOSAR team has trained more than 2,700 law enforcement officers at the federal, state, and local levels across the United States and globally. In 2022 alone, 216 officers underwent the two-day training program, comprising classroom and practical training segments.

The BOSAR Unit comprises 82 sworn members ranging from Trooper to Detective Lieutenant. It has been deployed operationally at numerous events throughout Massachusetts, leading to increased popularity and relevance in recent years. With the current local, national, and international climate, the BOSAR program's importance is expected to grow significantly in ensuring event security.

[redacted]

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

Cyber Crime Unit (CCU)

MISSION

The **Cyber Crime Unit** (**CCU**) conducts technical investigations. It provides digital forensic support for the search and seizure of digital evidence in all types of crimes, including homicides, sexual assaults, child exploitation cases, narcotics violations, financial crimes, and cyberstalking, among many others. The specially trained Troopers respond 24/7 for investigative and forensic missions. Unit members routinely become involved in some of the most highly technical, complex, and sensitive cases that law enforcement agencies encounter. The CCU supports Massachusetts State Police personnel and our local, state, and federal partners. Unit Troopers serve as Task Force Officers on the Homeland Security Investigations-Boston Cyber Crimes and Child Exploitation Group, the Federal Bureau of Investigation Child Exploitation Unit, the Federal Bureau of Investigation Regional Computer Forensic Laboratory, and the United States Secret Service Cyber Crime Task Force.

Digital Forensics

They also have a lead role in the Internet Crimes Against Children Task Force for Massachusetts. Cyber Crime Unit members, certified in digital forensics, are also dedicated to collecting, preserving, and analyzing computers and digital evidence. Forensic services include examining hard drives, removable media, cellular devices, mobile devices, GPS devices, wireless & Wi-Fi devices, and providing video surveillance capture and clarification of digital video files, web video, analog video, still cameras, or scanned images. The CCU will have a new Mobile Computer Forensics Van in early 2023, a fully equipped lab that allows Digital Forensic

Electronic Scent Detection (ESD) K-9

Examiners to respond 24/7 to preview and examine digital media on-scene in a sanitary lab environment. In January 2022, the newest member of the MSP CCU, ESD K-9, "Griffin," completed training through Jordan Detection K-9. K-9 Griffin joined CCU after being awarded to the Massachusetts State Police through the not-for-profit organization Operation Underground Railroad. K-9 Griffin is certified and capable of detecting many electronic storage devices, including DVDs, USB drives, hard drives, SD cards, and microSD cards. Trooper Benesh and K-9 Griffin have assisted on more than thirty (30) search warrants. Trooper Benesh and K-9 Griffin have also assisted New Hampshire ICAC with many search warrants.

INTERNET CRIMES AGAINST CHILDREN TASK FORCE

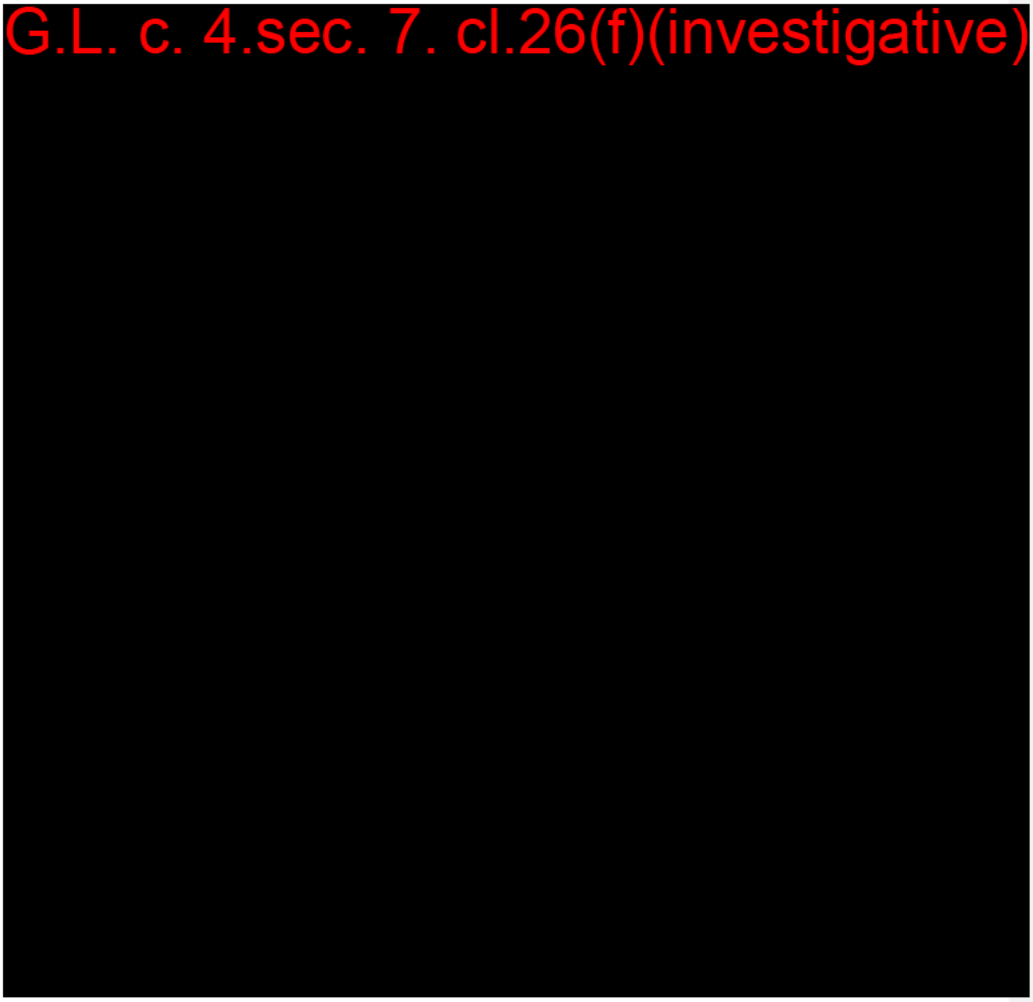
The MSP's Cyber Crime Unit operates the federally funded multi-agency **Internet Crimes Against Children** (**ICAC**) Task Force in Massachusetts, which helps state and local law enforcement agencies investigate predators who exploit and victimize children using computers and the Internet. The ICAC supports a multi-pronged strategy to combat online child exploitation, including undercover online investigations, nationwide investigation coordination, search warrant preparation and execution, investigative and analytical support, training for police officers and prosecutors, public awareness campaigns, and outreach activities to schools, parents, and community groups. As members of the national Internet Crimes Against Children Task Force, CCU members are often involved in some of the most heinous and sensitive investigations, referred to the CCU by the National Center for Missing & Exploited Children (NCMEC) in Virginia. The NCMEC refers CyberTipline reports to the MSP Cyber Crime Unit, which as the lead agency, is the clearinghouse for Massachusetts. The information gathered in the CyberTipline reports determines whether an investigation is warranted. Cyber tips sent to the Massachusetts ICAC Task Force have increased by over forty percent (40%) since 2021.

Cyber Crime Unit Activity, 2023	
Cybertip Investigations Opened	1,504
Search Warrants	152
Arrests/Criminal Complaints	92
CyberTipline Reports Received	9,532

Significant Activities and Investigations

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

[redacted]



Fraud Identification Unit

MISSION

The Fraud Identification Unit (FIU) is an investigative Unit working in concert with the Massachusetts Registry of Motor Vehicles. In 2022, the Unit was staffed with one Lieutenant and three Troopers. Members of this Unit conduct investigations related to the false procurement of official RMV documents, manage the RMV facial recognition program, investigate attempts to obtain RMV credentials fraudulently, investigate threats related to and crimes committed against RMV facilities or employees as well as investigate crimes committed

by RMV employees as they relate to their official duties. Members also investigate the misuse of personal information obtained through the RMV ATLAS database by RMV employees, insurance companies, car dealerships, etc., who have access to this information.

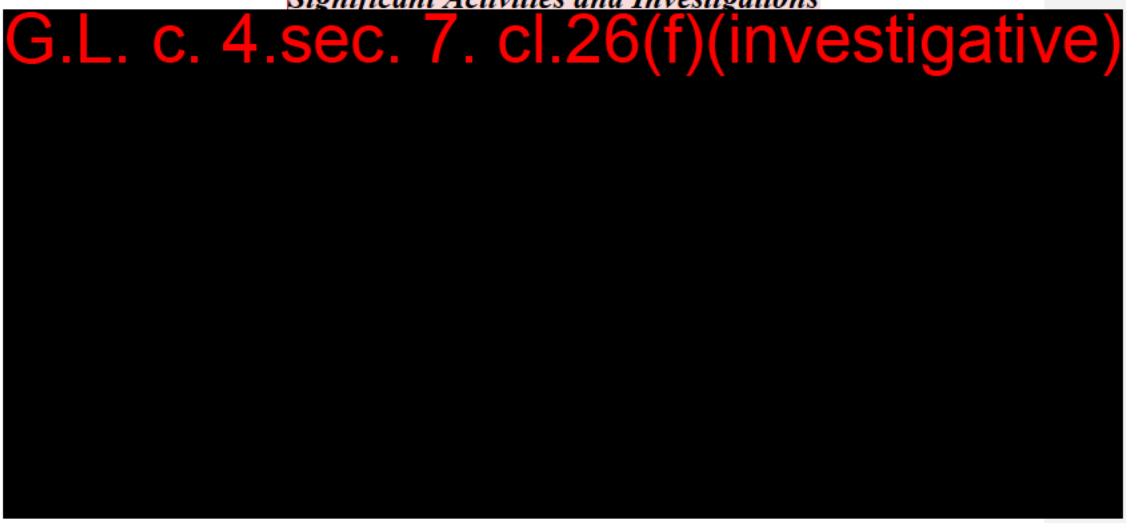
Further, members also assist local, state, and federal law enforcement agencies with collaborative investigations involving RMV documents, facilities, or employees. FIU works with the Alcoholic Beverages Control Commission when they discover a pattern of fraudulently obtained licenses for the underage purchase of alcohol, Homeland Security Investigations on their Document and Benefit Fraud Task Force, and the Department of Transportation Auditors on cases they uncover where there may be criminal activity on the part of RMV employees or where changes in RMV protocols may mitigate such activity.

Unit members participate in a multi-agency task force targeting the misuse of RMV-issued Handicapped Parking Placards. FIU members handle "State to State" cases forwarded by other state jurisdictions when a subject in another state is trying to obtain a credential using information already in existence in Massachusetts, or vice versa.

Fraud Identification Unit 2022 Activity

Arrests	**34**
Summons	38
Arrest Warrants Obtained	10
Facial Recognition Criminal Cases Generated	967
Assistance Rendered to Other Agencies	119
RMV Document Requests	174
State To State Investigations	69
External Facial Recognition Requests	13

Significant Activities and Investigations



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

State Identification Section (SIS)

MISSION

The State Identification Section (SIS) provides efficient and accurate real-time identification and criminal history services for law enforcement and specifically authorized civil applications to further public safety. SIS serves as the statewide repository of fingerprint records for arrests, sex offender registrations, deceased persons, license-to-carry applicants, and law enforcement and civilian employment applicants. SIS responsibilities include the following:

- Processing criminal records and fingerprint submissions for Statewide Applicant Fingerprint Identification Services (SAFIS), including teachers, social workers, DYS, and DCF, and processing fingerprint background checks for agencies issuing licenses.
- Managing court disposition updates, expungement orders, and court-ordered fingerprint-based criminal history records sealing.
- Assisting local police departments in procuring Livescan fingerprint devices, network configurations, and setups with DCJIS and vendors through grant funding.
- SIS has oversight of the latent print services for authorized forensic analysts in the Commonwealth. There are nine (9) agencies in the state with latent workstations.
- Criminal records in AFIS are utilized to confirm the identity of CODIS/DNA hits.
- SIS assists the OCME's offices across the state in identifying deceased individuals.

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

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

Unit Metrics

SIS received and processed 366,906 Ten Print (fingerprint) record submissions in 2022. This was an increase of 29,572 submissions from 2021. These submissions are broken down as follows:

- Criminal Arrests from Livescan booking and hard cards totaling 85,894
- Law Enforcement Applicants and CJIS Certification, totaling 7,384
- User fee applicants such as Firearms, Teachers, DYS, Gaming Commission, and Local Bylaw Applicants (ex., taxi drivers, ice cream vendors), totaling 226,033
- Sex Offender Registration totaling 611
- Criminal Inquiries, such as protective custody and victim ID, totaling 605
- Other, totaling 43,514 (includes 6,248 OCME portable Livescan submissions of deceased persons)
- The AFIS System provided 1,847 candidates at the state and FBI level that hit to latent prints entered by MSP CSSS and local agencies. An additional 75 candidates were provided as new fingerprint cards were entered into the AFIS system and hit on older, registered prints that had not provided prior identification to MSP CSSS and local agencies.

ACISS

Overview and Mission

The Division of Homeland Security and Preparedness continues to support all Divisions within the Organization with the use of the ACISS Application. ACISS is an acronym for 'Augmented Criminal Investigations Support System', which continues to meet the Department's needs. DIS, DHS, DST, and DAS utilize all aspects of ACISS, from case and lead management to telephone analysis. Initially procured as a solution to meet case management needs of DIS, the application has continued to mature, expanding its features, adding new functionality, and providing data integrations with other 3rd party applications. In 2022 funding was secured to expand ACISS and migrate the current user base to the AZURE Government Cloud environment. Throughout the year, work has progressed with representatives from EOTTS to assist with the technical aspects of this migration. ACISS was also provided funding to expand the applications user base to the Division of Field Services. This expansion and creation of a "Call Tracking" and "Mobile" platform are within the testing stages for future deployment with the Massachusetts State Police.

Evidence Systems Initiative (ACISS)

Members of the Office of the Division Commander for the Division of Homeland Security launched an initiative to update the Department's evidence storage and handling systems and procedures. The initiative will help the agency protect at-risk populations and civil rights by providing the procedural and technological best practices to ensure evidence is appropriately stored pre- and post-conviction. The initiative included evaluating, selecting, and purchasing equipment and technology and reviewing legal, professional, and policy standards. The installation of new evidence technology solutions in the Division of Field Services was completed in 2022. This initiative is ongoing, as evidence officers are trained and supported throughout the Divisions. The Division of Administrative Services, Long Term Evidence Unit also supports the ACISS Property and Evidence Initiative. Divisions within Investigation Services, Homeland Security, and Field Services now have a central location to store evidence that needs to be kept secure for extended periods of time.

Automatic License Plate Recognition Program (ALPR)

The Division of Homeland Security and Preparedness administers the Department's Automatic License Plate Recognition (ALPR) program. This system uses cameras to recognize the numbers and letters on the registration plates of passing vehicles and converts the image into characters that computer applications can process. The cameras can be temporarily deployed strategically for public safety events, mounted on cruisers, or affixed to structures near critical infrastructure

sites or major roadways. Over the course of 2022, the Department completed the transition of the ALPR system from an older, locally hosted server at DCJIS to a modern, cloud-based program. DHS staff reviewed the locations of ALPR sites to ensure that they were placed to provide maximum public safety benefits and provided training to system users on best practices and privacy considerations. The ALPR program provided increased security and situational awareness to support major public events such as the Boston Marathon and July 4th celebrations at the Esplanade. Over the past year, the Department used ALPR technology to solve or obtain critical investigative leads in a variety of public safety and criminal matters, including:

Success Stories

- Armed home invasion in Attleboro
- Human trafficking investigation involving juveniles from the Berkshires
- Identification of a vehicle used in the shooting of a female in New Bedford
- Arrest of a suspect wanted for attempted murder and sexual assault in South Carolina
- Identification of a vehicle that fled from a pursuit in Vermont
- Hit & run of a pedestrian with serious injuries in Springfield
- Arson of a business with injuries in Holyoke
- Bank robbery pattern in the Boston area
- AMBER alert and reported child abduction in Fall River
- Safe recovery of a missing endangered elderly male from Connecticut
- Identification and apprehension of a suspect in fatal hit & run of bicyclist in Holyoke

Air Wing

Overview and Mission

The State Police Air Wing provides statewide aviation support for all Massachusetts police, fire, and public safety operations. The unit operates twenty-four hours a day and is the most comprehensive public safety aviation unit in New England. The Air Wing operates four turbine powered helicopters and two fixed-wing airplanes. The helicopters are Airbus EC-135's and H-135's. They are equipped with state-of-the-art technology, allowing the crews to successfully complete various missions. The fixed-wing airplanes are a Cessna 182 and a Cessna Grand Caravan 208 EX. The Cessna 182 serves primarily as a training aircraft but can be used for photography and transportation missions. The Grand Caravan is a sophisticated aircraft for long-term surveillance, transportation, and searches.

In 2022, the Air Wing flew 1,578 missions totaling 1,780 flight hours. Nearly half of the missions were in support of local law enforcement agencies. These missions included searches for missing and wanted persons, surveillance and reconnaissance, aerial photography, SafetyNet,

firefighting, large crowd demonstrations/protests, motor vehicle pursuits, and ceremonial fly-bys. The Air Wing frequently responds to searches for wanted, missing, or endangered persons. The aircraft's FLIR (Forward Looking Infrared camera) is critical in locating these subjects. The camera's technology allows crew members to locate people in remote, concealed, or no light environments. The camera's video images can be transmitted to fixed-based receivers, allowing incident commanders to view real-time video to gain situational awareness and assessment during critical/tactical incidents, natural disasters, and large-scale public events. This allows viewers to see the video from any device with internet access. In October of 2022, the Air Wing received funding through the Homeland Security Grant Program to improve downlink capabilities in western Massachusetts. This funding will be used to install a fixed-base receiver in the Mt. Greylock area.

The Air Wing began to make improvements to the Department's helicopters through a previous Homeland Security Grant (Awarded in October 2021). The funding allows the department to replace aging mission equipment, including airborne monitors and recorders. These electronics are critical to the success of Air Wing missions. Upgrades are expected to be completed in Spring 2023.

In April 2022, the Air Wing took delivery of its newest helicopter. The Airbus H-135 is an improved version of the current EC-135. The aircraft's state-of-the-art cockpit includes a four-axis autopilot, providing additional safety measures for flight crews. It is also equipped with the most advanced mapping system, FLIR camera, police radios, microwave downlink, and other mission-critical components. This technology will increase Air Wing mission success and efficiency.



Air 2 (New H-135) at Gillette stadium.

ACISS

The Division of Homeland and Security and Preparedness continues to support all Divisions within the Organization with the use of the ACISS Application. ACISS continues to meet the Departments needs by DIS, DHS, DST and DAS utilize all aspects of ACISS, from case and lead management to telephone analysis. Initially procured as a solution to meet case management needs of DIS, the application has continued to mature, expanding its features, adding new functionality and providing data integrations with other 3rd party applications. In 2022 funding was secured to expand ACISS and migrate the current user base to the AZURE Government Cloud environment. Throughout the year, work has progressed with representatives from EOTTS to assist with the technical aspects of this migration. ACISS was also provided funding to expand the user base of the application to the Division of Field Services. This expansion and creation of a "Call Tracking" and "Mobile" platform is within the testing stages for future deployment with the Massachusetts State Police.

Evidence Systems Initiative (ACISS)

Members of the Office of the Division Commander for the Division of Homeland Security launched an initiative to update evidence storage and handling systems and procedures across the Department. The initiative will help the agency protect at-risk populations and civil rights by providing the procedural and technological best practices needed to ensure that evidence is properly stored pre- and post-conviction.

The initiative included evaluation, selection and purchase of equipment and technology; reviews of legal, professional and policy standards. The installation of new evidence technology solutions in the Division of Field Services was completed in 2022. This initiative is ongoing, as evidence officers are trained and supported throughout the Divisions. The ACISS Property and Evidence Initiative is also supported by the Division of Administrative Services, Long Term Evidence Unit. Divisions within Investigation Services, Homeland Security and Field Services now have a central location to store evidence that needs to be kept secure for longer periods of time.

Automated License Plate Reader Program (ALPR)

The Division of Homeland Security and Preparedness continues to implement and roll out a network of Automated License Plate Reader (ALPR) cameras across the Commonwealth. These cameras capture the numbers and letters located on the registration plate of a vehicle and convert the image into characters that can be processed by various computer applications. This technology has been successfully used in a variety of public safety and criminal matters to include: missing persons, child abduction and AMBER Alerts, crimes of breaking and entering, homicide, opiate trafficking, stolen and wanted vehicles and Silver Alerts. The cameras can be strategically placed for a particular area in which a crime may have occurred, mounted on cruisers or permanently mounted at major traffic locations.

The Commonwealth Watch Center is a vital component of the ALPR program and monitors and maintains the "hot lists" into which the registration plate(s) in question are entered. The Watch Center communicates with police partners across the Commonwealth as well as other states throughout the country, that have a public safety or criminal investigation nexus to a registration plate. Watch Center

staff are also available to assist investigators by communicating with other states that have similar technology that may help recover a missing person or solve a crime in Massachusetts.

The current Massachusetts policy allows for data retention for a one-year period at which point it is expunged; New York and New Jersey currently store their ALPR data for five years. DHS recently attended a two-day meeting held in New Jersey and New York City in which the sharing of this information among several east coast police agencies, was discussed.

41.3.9	License Plate Readers	ACCREDITATION Mandatory	Revision Date: 09/15/2022	Written Directive Written Documentation
Note to Accreditation Managers and Assessors				Proofs of Compliance
This standard requires written guidelines for the use of License Plate Readers (LPR's) and establishes the responsibilities of the LPR Operator.				❑ Written Directive ❑ Documentation of Operator Training

STANDARD / EVALUATION MEASURES:

1. The agency utilizes License Plate Readers (LPRs). **Y N**

If **No**, the agency provided a WAIVER conditionally approved by the Commission's Executive Director.
Y N

If **Yes**, the standard applies to the agency and the following info in the below table must be met.

2.	The agency has a written directive governing the use of License Plate Readers.	**Y N**
3.	The written directive addresses:	
A	Guidelines for use	**Y N**
B	Operator responsibilities	**Y N**
C	Operator training	**Y N**
D	Data entries	**Y N**
E	Data storage and security	**Y N**
F	Access to data	**Y N**
G	Data retention	**Y N**
4	Agency provided documentation demonstrating LPR Operators received required training. Name(s) sampled:	**Y N**

Policy Changes – Privacy Protection Highlights

- Hotlist manual entries:
  - Hot plate max allowable time reduced from 1 year to 30 days (not system retention)
  - Added requirement for supervisory approval to hotlist a plate
  - Added notice that user requested hotlist add must also remove it
  - Added special attention to rental and short-term use vehicles;
  - Added special attention to incidents that may be quickly resolved;
  - Added that entries must be for the shortest time necessary or reasonable;

- Search guidelines section:
  - Introduced and revised privacy protection guidelines
  - Added requirements to limit temporal and geographic parameters of search
  - Added that we may deny requests believed to be overly intrusive or otherwise improper

- Added legal considerations section:
  - discussion of McCarthy opinion and legal factors
  - suggestion to consult with ADA for longer term use

- Allowable/prohibited uses:
  - Added restriction against system use for immigration enforcement
  - Several other language modifications to improve clarity and specificity

- Records preservation and discovery:
  - Added explicit requirement to preserve or export reports for discovery prior to expiration

- Outside LPR systems:
  - Added requirement that that tightly restricts access to outside systems
  - Access to outside systems is limited essentially to watch/fusion center & ALPR admin
  - Added cautionary notice on different technology/retention of outside systems.
  - All searches of outside systems must also otherwise comply with MSP policy for its own system

- Training & Privacy:
  - Added requirement that all users receive training to include best practices and privacy considerations

- Other relevant updates:
  - Improved and clarified section on verifying an LPR hit prior to taking any enforcement action for field cruisers

Commonwealth Fusion Center
Standard Operating Procedure

Effective Date	Number
April 4, 2023	CFC- 12

POLICY FOR THE UTILIZATION OF VIDEO SYSTEMS IN THE COMMONWEALTH WATCH CENTER

GENERAL

The availability and use of video at the Commonwealth Watch Center provide opportunities for enhancing security for the Commonwealth's infrastructure, major events, government agencies, and coastal maritime and port operations. The use of video systems increases the productivity and effectiveness of law enforcement and public safety agencies and provides opportunities to increase officer and public safety.

It is the policy of the Department of the State Police (Department) to respect the privacy interests of all persons in the Commonwealth. The Watch Center shall only utilize video systems in furtherance of official and legitimate law enforcement operations and public safety or security and shall comply with all applicable laws and Department Policies and Procedures, Rules and Regulations, Fusion Center, and/or unit-specific operating procedures.

PURPOSE & APPLICABILITY

A. To establish guidelines and procedures for the proper use and application of video systems utilized by the Commonwealth Watch Center.

B. To provide guidelines and principles for collecting, accessing, disseminating, and retaining video system recordings, data, and information.

C. To ensure that such recordings, data, and information are used for legitimate law enforcement purposes and that individuals' privacy, civil rights, and civil liberties are not violated.

D. Excluding Cruiser Mounted Cameras and Body Worn Cameras governed by ADM-35 and Automatic License Plate Recognition (ALPR) technology governed by TRF-11, this policy applies to any and all live-feed video systems, with or without video recording capabilities, accessible within the Commonwealth Watch Center, including, but not limited to:

(1) Department Video Systems;

(2) External Video Systems;

(3) Massachusetts Coastal Maritime Security Video System (CMSVS);

(4) MassDOT Highway Cameras; and

(5) Any additional live-feed video systems, with or without video recording capabilities, utilized on a long-term or temporary basis including instances such as covert operations, special events, or demonstration/trial purposes.

DEFINITIONS

Department Video Systems: All video camera systems operated and maintained by the Department with live-feed viewing, with or without video recording capabilities, but not limited to, Department-operated building and infrastructure security camera systems and video cameras operated by the MSP Air Wing with the ability to provide live-feed video or imagery, with or without recording capabilities, through the use of aviation aircraft and unmanned aerial vehicles (UAVs), but excluding Cruiser Mounted Cameras and Body Worn Cameras as governed by ADM-35 and Automatic License Plate Recognition (ALPR) technology as governed by TRF-11

External Video Systems: All video camera systems operated and maintained by agencies, municipalities, or private entities outside of the Department that provide the Commonwealth Watch Center with live-feed video or imagery with or without video recording capabilities.

Live-Feed Video or Imagery: All video or images, digital or analog, streamed or transmitted from a live, not recorded, source.

Grant Provisions: The provisions of the U.S. Department of Homeland Security / Federal Emergency Management Agency Port Security Grant (Sub Account No. EMW-2020-PU-0056) awarded to the Massachusetts Executive Office of Public Safety and Security (EOPSS), effective on July 1, 2022, and any/all subsequent related grants or award(s).

Massachusetts Coastal Maritime Security Video System (CMSVS): A U.S Department of Homeland Security / Federal Emergency Management Agency grant funded, Executive

Office of Public Safety and Security secure network of port and maritime security cameras connected to an isolated server designed to be both interoperable with existing Department of Homeland Security Urban Security Initiative and United States Coast Guard camera systems and accessible to participating federal, state, and municipal agencies.

MassDOT Highway Cameras: A Massachusetts Department of Transportation video camera system providing live-feed video or imagery, with or without recording capabilities, of highways, roadways, and other location points throughout the Commonwealth.

ADMINISTRATION & OPERATION

A. The Department shall manage, maintain, and oversee all Department video systems. Department equipment, recordings, data, and information shall be acquired, processed, maintained, disseminated, and/or disposed of in accordance with this policy, Department policy, Fusion Center Standard Operating Procedures, grant provisions, and all applicable laws.

B. External video systems shall be managed, maintained, and overseen by the respective agencies and municipalities responsible for such systems. External video system recordings, data, and information shall be acquired, processed, maintained, disseminated, and/or disposed of in accordance with any applicable agreement with the entity responsible for each external video system as well as this policy, Department policy, Fusion Center Standard Operating Procedures, grant provisions, and all applicable laws.

C. The Department shall, as delegated by the Colonel or a designee and on behalf of and by agreement with EOPSS, manage, maintain, and oversee CMSVS. CMSVS equipment, recordings, data, and information shall be acquired, processed, maintained, disseminated, and/or disposed of in accordance with this policy, Department policy, Fusion Center Standard Operating Procedures, grant provisions, and all applicable laws.

AUTHORIZED ACCESS AND USES

A. Access to video systems viewable at the Commonwealth Watch Center that are not available to the general public shall be restricted to authorized Watch Center employees, Fusion Center employees, Department employees with Watch Center access, and other individuals authorized by the Commonwealth Watch Center supervisor, Fusion Center Commander, Division Commanders, or the Colonel or designee.

B. Use of video systems viewable at the Commonwealth Watch Center video is strictly limited to law enforcement and public safety purposes only. The following are valid law enforcement and public safety purposes:

(1) Preventing, monitoring and/or mitigating any threat to infrastructure, government, homeland security, port or coastal security, major events, law enforcement, or public health and safety;

(2) Supporting law enforcement and public safety agencies during major events, critical incident responses, and exigent circumstances;

(3) Criminal investigations;

(4) Crime analysis; and

(5) Criminal intelligence gathering.

C. Watch Center personnel and other authorized users shall not utilize video systems to monitor or gather information about:

(1) Individuals or organizations solely on the basis of their religious, political, social views or activities; or

(2) An individual's or organization's participation in a particular non-criminal organization or lawful event; or

(3) An individual's age, race, ethnicity, religion, citizenship, place of origin, disability, gender, gender identity, genetic information, or sexual orientation unless such information is relevant to the individual's criminal conduct or activity or if required to identify the individual.

RESTRICTED USES & LIMITATIONS

A. Transmitting or recording audio on a Commonwealth Watch Center video device is strictly prohibited. Due to the possibility of violating legitimate privacy expectations, inadvertently recording protected conversations, or unintentionally violating M.G.L. c. 272, §99 (Interception of Wire and Oral Communications), all Commonwealth Watch center video system devices shall be configured so they do not transmit or record audio unless otherwise permitted by law.

B. Using or requesting the use of Commonwealth Watch Center video systems for personal use is strictly prohibited and considered employee misconduct as well as a violation of this policy.

C. Commonwealth Watch Center video equipment and technology shall not be intentionally used for viewing, recording, or transmitting images or video in a criminal investigation at any location or property where a person has a reasonable expectation of privacy unless:

(1) A warrant or court order has been approved for the search of the property;

(2) Consent by the owner or person responsible for the property is obtained; or

(3) Exigent circumstances exist, including but not limited to: search and rescue missions, tactical missions, crash/accident scenes, crime scenes, fire scenes, hazmat scenes and/or natural disasters.

PROSECUTORIAL & COURT ORDERED RESTRICTIONS

Commonwealth Watch Center video system recordings, data, and information are subject to state and federal laws and any court of competent jurisdiction orders. Video recordings shall be preserved, stored, and retained in accordance with the requests, directions, and orders of appropriate prosecutorial and/or judicial authorities.

PRESERVATION OF VIDEO SYSTEM DATA

All Commonwealth Watch Center video system recordings, data, and information shall be processed, maintained, disseminated, preserved and/or destroyed in accordance with applicable Department and/or Fusion Center policies and procedures, including but not limited to those concerning public records, privacy, and the preservation of evidence.

Promulgated By:

Division of Homeland Security and Preparedness

Criminal Information and Intelligence Section

Inside the Commonwealth Fusion Center

March 2021

MCSAP Qualifying Conditions Review

State of: Massachusetts **Date Completed:** 1/25/2023

FMCSA Representative: John Toto **Phone:** 857-292-3122 **Email:** john.toto@dot.gov

State Representative (1): Lt Vincent Noe **Phone:** 781-858-3708 **Email:** Vincent.noe@state.ma.us

State Representative (2): **Phone:** **Email:**

Instructions:

1) Complete the questionnaire using the information from the most recent submitted eCVSP for FY 2021.
2) If you need to attach materials to support an answer, in the box provided please reference the attachment and identify where the information is located in the attachment (e.g., page number, legislative citation, etc.).
    a. It is only necessary to attach information relevant to the review, e.g. for omnibus safety bills, it is only necessary to provide the relevant MCSAP sections and not the entire bill.
3) If more space is needed to complete the questions, include additional information in a separate document.
4) If you have any questions about the review, contact your Division office.
    a. The User Guide provides details about the process, timeline, and next steps.

Item No.	Federal Regulation or Policy	Question/Topic	Yes/ No	Comments/Explanation
1.	350.207(a)(1)	Does the State document have the designation of Lead State Agency? If yes: Provide the document. If no: Explain.	YES	The MSP has been the lead Agency since the inception of the MCSAP Program and have not had any change in designation since that time.
2.	350.207(a)(2)	Does the State assume responsibility for improving motor carrier safety by adopting and enforcing compatible safety laws and regulations, standards, and orders, except as may be determined by the Administrator to be inapplicable to a State enforcement program?	YES	The State has certified via their eCVSP. The State has adopted all regulations identified as: *540CMR14.03 and 540CMR14.04*
3.	350.207(a)(3)	Does the State ensure cooperation in the enforcement of financial responsibility requirements under part 387? If yes: Provide the State statute or regulation that allows enforcement of financial responsibility requirements. If no: Explain.	YES	The State has the regulatory authority under 540CMR14.04. The State utilizes their INSPECT program, which gives them the ability to check a for-hire Carrier's compliance with Part 387 and the roadside protocol requires the Troopers to check Insurance cards. Additionally, the State utilizes their access to Query Central and CVIEW to check operating authority to ensure the Carrier has the correct amount of financial responsibility. The State conducts New Entrant Audits and verifies the Carrier has the proper insurance by requesting copies of their MCS-90 Financial Endorsement. The State does not conduct CR's at this time.

Item No.	Federal Regulation or Policy	Question/Topic	Yes/ No	Comments/Explanation
4.	350.207(a)(4)	Does the State enforce the registration requirements under 49 U.S.C. 13902 and 31134 by prohibiting the operation of any vehicle discovered to be operated by a motor carrier without a registration issued under those sections or operated beyond the scope of the motor carrier's registration? If yes: Provide the State statute or regulation that permits enforcement of registration requirements. If no: Explain.	YES	540CMR2 Massachusetts is in full participant in the PRISM program. The protocol for the Roadside Inspectors who are State Troopers is to interview the driver, verify registration requirements through their access with Inspect, the software program used to complete Roadside inspections. The Trooper will utilize L&I through the portal to verify compliance as well. If a Carrier is determined to be violating an OOS order, while in Interstate commerce, the Trooper takes appropriate action by placing the driver/carrier OOS.
5.	350.207(a)(5)	Does the State provide a right of entry (or other method a State may use that is adequate to obtain necessary information) and inspection to carry out the CVSP? If yes: Provide the State statute or regulation that permits right-of-entry inspections. If no: Explain.	YES	Under M.G.L 90-19L
6.	350.207(a)(6)	Does the State give satisfactory assurances in its CVSP that the Lead State Agency has the legal authority, resources, and qualified personnel necessary to enforce compatible safety laws and regulations, standards, and orders?	YES	The State uses sworn State Troopers who have the power of constables and police officers throughout the Commonwealth of MA. All MCSAP Troopers are trained in the North American Part A, B, General HM and are required to maintain their certification as required in CVSA Policy. The MSP CVES unit conducts in-service training and conducts weekly audits of their personnel to ensure compliance with Part 350. Under statute authority granted to them in M.G.L. 90-19L, they have the authority to conduct SA's, CR's and inspections.

7.	350.207(a)(7)	Does the State provide satisfactory assurances that the State will undertake efforts that will emphasize and improve enforcement of State and local traffic laws and regulations related to CMV safety?	YES	*MA works with UMassSafe on mapping the high crash corridors in the state and then patrols are directed to conduct enforcement in those areas.* *The State has conducted 5,063 traffic enforcement initiatives inspections ytd out of a projected 10,000 inspections. The state participates in Operation Road check and Operation Safe Drive each year. The state also conducts enforcement blitzes throughout the state several times a year.*

Item No.	Federal Regulation or Policy	Question/Topic	Yes/ No	Comments/Explanation
8.	350.207(a)(8)	Does the State give satisfactory assurances that the State will devote adequate resources to the administration of the CVSP throughout the State, including the enforcement of compatible safety laws and regulations, standards, and orders?	YES	*The Colonel of the MSP signs and certifies the CVSP. MSP monitors any progress or changes to any proposed legislation.* *The Commercial Vehicle Enforcement Section for the MSP currently has 24 full-time troopers assigned to it. These troopers are assigned throughout the state. CVES deploys its troopers to high crash corridors daily to conduct enforcement.* *CVES has recently added and trained 15 part-time troopers to assist with conducting traffic enforcement throughout the state.* *CVES currently has 1 Sergeant and 1 Trooper assigned to New Entrant Audits full-time and 5 additional troopers doing to on a part-time basis.*
9.	350.207(a)(9)	Does the State provide that the MOE of the Lead State Agency will be maintained each fiscal year in accordance with 49 CFR 350.225?	YES	The Massachusetts State Police maintains MOE through expenditures for vehicles, vehicle maintenance and parts, law enforcement equipment & supplies, facility infrastructure maintenance & repair, and fuel for vehicles and buildings.
10.	350.207(a)(10)	Does the State provide that all reports required in the CVSP be available to FMCSA upon request, meet the reporting requirements, and use the forms for recordkeeping, inspections, and investigations that FMCSA prescribes?	YES	*Fully Cooperative.*

11.	350.207(a)(11)	Does the State implement performance-based activities, including deployment and maintenance of technology, to enhance the efficiency and effectiveness of CMV safety programs?	YES	*The state is currently installing aLPR's on all cruisers assigned to the commercial vehicle unit. The state works with UmassSafe on current crash trends and high crash areas throughout the state. The state is in the process of purchasing and installing Tire anomaly systems at inspections site around the state.* *During each inspection troopers run the driver and DOT# through CVIEW.*
12.	350.207(a)(12)	Does the State establish and dedicate sufficient resources to a program to ensure that accurate, complete, and timely motor carrier safety data are collected and reported, and to ensure the State's participation in a national motor carrier safety data correction system prescribed by FMCSA?	YES	*We monitor data quality standard monthly and make corrections to as needed to stay in the green. The State utilizes a full-time data analysist to monitor data quality and ensure crash/inspection accuracy. The State also answers all Data-Qs in a timely manner. The State has received 410 Request to review in the past 365 days. The State has processed these reviews on average within 10 days of the Data Q request. At this time the reviews are being processed and adjusted by Lt. Noe.* *Good Rating*
13.	350.207(a)(13)	Does the State ensure that the Lead State Agency will coordinate the CVSP, data collection, and information systems with the State highway safety improvement program under 23 U.S.C. 148(c);	YES	*Fully participate in the SHSP planning and development. Lt. Noe is the chair of the large truck portion of the states SHSP.*
14.	350.207(a)(14)	Does the State ensure participation in information technology and data systems as required by FMCSA for jurisdictions receiving MCSAP funding;	YES	*Yes, Massachusetts had deployed Inspect for roadside inspections and CVIEW, which both interface with FMCSA systems. They also complement the software that FMCSA deploys, All MCSAP personnel have portal accounts that allow for access to all software, namely MCMIS, ACE, QC, Safer, NEWS, CAPRI, A&I, Data-Q and AIM. MCSAP personnel are required to utilize these systems to verify Carrier status, conduct NE audits, complete Data-Q requests and MSP utilizes Safety net to ensure timeliness uploads of Crash and Inspection.*

Item No.	Federal Regulation or Policy	Question/Topic	Yes/ No	Comments/Explanation
15.	350.207(a)(15)	Does the State ensure that information is exchanged with other States in a timely manner;	YES	*We provide states with what they need upon request. Always in a timely manner. The State SSDQ is currently in the green with a good rating. Crash record timeliness is at 92% and Inspection Upload timeliness is at 100%.* *State is in Green rating.*

16.	350.207(a)(16)	Does the State grant maximum reciprocity for inspections conducted under the North American Standard Inspection Program through the use of a nationally accepted system that allows ready identification of previously inspected CMVs?	YES	The MSP issues CVSA decals pursuant to the CVSA Operational Policy after a successful completion of a Level 1 inspection with no critical defects. All MCSAP personnel are trained in the proper issuance along with training in identifying vehicles that have a current and valid decal. The Division office has conducted a sampling of Level 1 inspections to verify compliance with this policy. Interviews were conducted with three MCSAP personnel to determine their understanding of the policy and gain an understanding of when they issue a decal.
17.	350.207(a)(17)	Does the State conduct comprehensive and highly visible traffic enforcement and CMV safety inspection programs in high-risk locations and corridors?	YES	*We work with UMassSafe on mapping high-risk corridors and direct patrols to conduct enforcement of those areas.*
18.	350.207(a)(18)	Does the State ensure that driver or vehicle inspections will be conducted at locations that are adequate to protect the safety of drivers and enforcement personnel?	YES	*Yes, we work with MassDOT to maintain function and cleanliness of the states weigh stations/Inspection sites where Level 1 inspections are conducted. The State may also conduct a roadside inspection other than a Level 1 on rural roads and highways when performing traffic enforcement and consistent with the training received in Part A North American Inspector Course that all MCSAP personnel took and are certified. Refresher training is also conducted on a quarterly basis. The MSP has a policy on conducting MV stops. This has been provided.*
19.	350.207(a)(19)	Except in the case of an imminent or obvious safety hazard, does the State ensure that an inspection of a vehicle transporting passengers for a motor carrier of passengers is conducted at a bus station, terminal, border crossing, maintenance facility, destination, or other location where a motor carrier may make a planned stop (excluding a weigh station)?	YES	*Yes, we conduct regular passenger CMV enforcement at destination locations, like Logan airport and South Station. There are times when passenger carriers may be stopped roadside for an unsafe traffic infraction and care is taken to select a safe and reasonable location to maximize safety of everyone.*

20.	350.207(a)(20)	Does the State provide satisfactory assurances that the State will address activities in support of the national program elements listed in Sec. 350.203, including activities? (i) Aimed at removing impaired CMV drivers from the highways through adequate enforcement of regulations on the use of alcohol and controlled substances and by ensuring ready roadside access to alcohol detection and measuring equipment;	YES	*Every Trooper conducting CMV inspections is certified in field sobriety and the used of Portable Breath Test machines. Also, majority of the troopers are Advanced Roadside Impaired Driving Enforcement. (ARIDE) Our eCVSP outlines initiatives and additional taskforces projected during our 3-year plan and demonstrates our compliance with the NRSS.* *During FY2022, we identified 73 violations of 392.4 and the violations were noted on roadside inspections.*
21.		(ii) Aimed at providing training to MCSAP personnel to recognize drivers impaired by alcohol or controlled substances; and	YES	*All troopers are trained and certified*

Item No.	Federal Regulation or Policy	Question/Topic	Yes/ No	Comments/Explanation
22.		(iii) Related to criminal interdiction, including human trafficking, when conducted with an appropriate CMV inspection and appropriate strategies for carrying out those interdiction activities, including interdiction activities that affect the transportation of controlled substances (as defined in section 102 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 802) and listed in 21 CFR part 1308) by any occupant of a CMV.	YES	*We are planning a joint operation with the MSP Human Trafficking Unit. The Human Trafficking Unit will deploy to the weigh stations with CVES troopers. All MCSAP certified Troopers handle these investigations and are trained as required.*
23.	350.207(a)(21)	Does the State ensure that detection of criminal activities and size and weight activities described in 350.227(b), if financed through MCSAP funds, will not diminish the effectiveness of the development and implementation of the programs to improve motor carrier, CMV, and driver safety?	YES	The state has personnel that are dedicated to size and weight enforcement. Criminal activity enforcement is conducted as needed and typically from a result of an CMV inspection. This does not impact the CVSP.
24.	350.207(a)(22)	Does the State ensure consistent, effective, and reasonable sanctions?	YES	*Fines are set by state statue. In FY2022 the state conducted 14,639 inspections. 11,903 resulted in a warning and 2,736 resulted in a citation being issued.*

25.	350.207(a)(23)	Does the State include information on best practices for driving safely in the vicinity of CMVs and non-CMVs in the training manuals for the licensing examinations to drive a CMV and non-CMVs? If yes: Provide a copy of the training manual for the licensing examinations. If no: Explain.	YES	Mass RMV driver manual
26.	350.207(a)(24)	Does the State require all registrants of CMVs to demonstrate their knowledge of applicable FMCSRs, HMRs, or compatible State laws or regulations, standards, and orders?	YES	*In MA all CMV's are required to have DOT numbers regardless of Interstate or Intrastate. They must affirm they know the rules.* *540CMR14.00*

Item No.	Federal Regulation or Policy	Question/Topic	Yes/ No	Comments/Explanation
27.	350.207(a)(25)	Does the State transmit to inspectors the notice of each Federal exemption granted under subpart C of part 381 and Sections 390.23 and 390.25 of this subchapter that relieves a person or class of persons in whole or in part from compliance with the FMCSRs or HMRs that has been provided to the State by FMCSA and identifies the person or class of persons granted the exemption and any terms and conditions that apply to the exemption? If yes: Provide a copy of the notice of exemptions sent to inspectors. If no: Explain.	YES	This is emailed to all the troopers in the Commercial vehicle enforcement section of the MSP. Email provided

28.	350.207(a)(26)	Does the State conduct new entrant safety audits of interstate and, at the State's discretion, intrastate new entrant motor carriers in accordance with subpart D of part 385?	YES	The State conducts New Entrant audits on Interstate carriers only at this time. MA has 74 Overdue Onsite audits and 248 Offsite audits. The State utilizes one Two Troopers full-time and five part time Troopers to actively conduct New Entrant audits and works closely with the Division office to ensure prioritization of overdue and expedited action audits.
29.	350.207(a)(27)	Does the State participate fully in PRISM by complying with the conditions for full participation, or receiving approval from the Administrator for an alternative approach for identifying and immobilizing a motor carrier with serious safety deficiencies in a manner that provides an equivalent level of safety? If yes: Identify current PRISM participation level. If no: Explain.	YES	The State of MA is participating in the Enhanced Participation and working on Leveling Up to Expanded.

Item No.	Federal Regulation or Policy	Question/Topic	Yes/ No	Comments/Explanation
30.	350.207(a)(28)	Does the State cooperate in the enforcement of hazardous materials safety permits issued under subpart E of part 385 of this chapter?	YES	*Troopers are given North American HM training and certification along with refresher training. Use MCMIS database to access validity of permit during roadside. This done as part of every inspection.*
31.	350.207(a)(29)	*Applies only to Border States; skip to question #32 if not applicable.* Does the State conduct a border CMV safety program focusing on international commerce that includes enforcement and related projects, or forfeit all funds allocated for border-related activities?	N/A	N/A
32.	350.207(b)	Does the State use third parties to conduct new entrant safety audits?	No	*N/A*

33.		Does the agency maintain a copy of the required Title VI plan and other documents, policies, procedures, etc. related to Title VI requirements?	YES	Lt. Vincent Noe is the POC of this document. The document has been sent and reviewed by all troopers assigned to the unit. The document is maintained at the CVES office and the MSP legal section.

MAURA T. HEALEY
GOVERNOR

KIMBERLY DRISCOLL
LIEUTENANT GOVERNOR

TERRANCE M. REIDY
SECRETARY

The Commonwealth of Massachusetts
Department of State Police

Division of Investigative Services
Violent Fugitive Apprehension Section
450 Worcester Road
Framingham, MA 01702

JOHN E. MAWN JR.
COLONEL/SUPERINTENDENT

JOHN D. PINKHAM
DEPUTY SUPERINTENDENT

August 03, 2023

To: Lieutenant Colonel Brian P. Connors, #2145, Division Commander, D.I.S.
Lieutenant Colonel Mark D. Cyr, #2728, Division Commander, DHS
Major Michael E. Farley, #2352, Deputy Division Commander, D.I.S.
Detective Captain Eric Benson, #3389, Executive Officer, D.I.S.

From: Detective Lieutenant John B. Sullivan, #3359, Unit Commander, V.F.A.S.

Subject: Permission for V.F.A.S. to Utilize Flock Safety ALPR's

1. "Flock Safety" is the name of the company. It's an American Company that basically sells ALPR technology to law enforcement agencies and neighborhood associations. Flock's cameras read license plates and send instant alerts to law enforcement officers based on a populated list. (Stolen cars, vehicles of interest). Unlike many other ALPR Systems, Flock camera's allow searches based on the car's color and various other visual features. TFR-11 addresses **"Use of Non-Departmental ALPR Systems"** of page 5 (of 8)**.** The policy allows MSP members to contact other agencies to request assistance with information. Additionally, the policy states that that supervisors and analysts from Watch Center & ALPR Administrator can access non departmental systems. However, the policy specifically states that other members shall not obtain/utilize accounts without permission from the Division Commander of the Division of Homeland Security and Preparedness.

2. V.F.A.S. members, respectfully, would like to continue utilizing Flock Accounts for fugitive investigations. Revere PD has voluntarily set up accounts for the Metro Guys and a member of VFAS North is able to utilize Lynn PD's Flock Account because he was a former Lynn Police Officer. Each account has a unique sign in (Job email address & strong password) to access the data and each user leaves a footprint. Currently, the Flock Map lists Quincy, Lynn, Revere, Winthrop, Everett & Malden as participating agencies. Each local police department has an administrator for Flock & that Admin. can asked permission (via email) to view participating agencies Flock Cameras. As recent as last Sunday (July 30, 2023), A member of V.F.A.S. Metro was able to utilize the Winthrop Flock Camera to apprehend a career violent felon who was wanted for a stabbing that occurred in Revere.

3. Members of V.F.A.S. are not using Flock ALPRs to develop PC or in the furtherance of an ongoing investigation/case. Flock has been a proven successful tool in multiple fugitive investigations assisting the apprehension of multiple violent felons. Additionally, per M.S.P. policy, V.F.A.S. gets called for Ambert Alert Activations and other exigency type cases that are time sensitive and Flock information can be obtained independently by investigating officers. Thank you for consideration in this matter.

Respectfully Submitted,

DLT. John B. Sullivan

John B. Sullivan, #3359
Detective Lieutenant, V.F.A.S.

State of Massachusetts benefits of LPR on MA DOT Roadways:

- AMBER Alert, Silver Alert, kidnapping/abductions, and other public safety and real-time emergency capabilities. (*i.e., recent Mass Shooting in Maine*)

- Investigation and prevention of terrorism and the protection of critical infrastructure and public events such as the Boston Marathon, and the investigation of major crimes and critical incidents.

Safeguards:

- Lawful use only with respect to privacy considerations, MSP carefully limits and monitors system use, follows all applicable laws, and has a thorough and up-to-date policy on ALPR use. (*ref. General Order TRF 11*)

Current uses:

- Successful (MSP / MA DOT) partnership exists. We have previously co-located LPR equipment with MA DOT on the Cape Cod Bridges since 2014.

- MSP has historically used solar trailers for other highway-based equipment needs; however, weather-related power problems have resulted in outages with missed important public safety information.

Request:

- MSP is asking for MA DOT to provide access only to existing state-owned infrastructure on MA DOT-managed highways. (No installation cost - MSP will install equipment on sites acceptable to MA DOT)

- Power draw, equipment weight, and footprint are very limited. No new construction or structural modifications are requested.

Macrimenet: Overview of Activities and Responsibilities

- Intake, review, edit and redistribution of incoming email and outgoing intelligence-related email for distribution to upwards of 2,000 individual recipients 365 days a year.
- Annual selective distribution by county, of approximately 4,000 emails to the email network which includes representatives of almost every State, Local and Federal Agency in Eastern and Central MA, neighboring states, Bank Industry Security Professionals and Retail Asset Protection Professionals.
- CFC Liaison to Area Detective's Meetings providing notification, invitation and published bulletins covering crimes and arrests of regional significance.
- Comprehensive review and re-distribution in excel spreadsheet format of Pawnshop Information provided by more than a dozen local agencies including highlighting of persons of interest.
- Statewide liaison to NABI (National Association of Bunco Investigators)
- Review and redistribution of Intelligence published by NESPIN and NEORCA.
- Complete responsibility for the addition, subtraction and update of email addresses stored in the 'listserv manager".
- Maintenance, upkeep and distribution of a home-grown Area Wide Detectives Contact List with email and telephone contact information from 1,800 sources.
- Routine access to CJIS systems to perform RMV, CJIS and NCIC related inquiries pertaining to email traffic.
- Routine access to Coplink and other data sources (TLO) to assist local detectives in providing photographs, known associates, associated vehicles and prior incidents while assisting in investigations pertaining to email traffic.
- Routine access and review of ALPR's to provide investigative assistance and documentation to local Law Enforcement, specifically in connection with Organized Crime organizations based out of State but operating in MA and the surrounding New England States.
- Daily review of Area Crime Bulletins from municipal agencies including the BRIC, Cambridge, Everett, Lynn, and others as they are distributed. (Many of whom re-post information previously distributed on Macrimenet).
- Guest presenter to New Area Detectives providing an overview of what services the CFC provides for local Law Enforcement.
- Liaison/conduit to announce and assist in coordination of area Intelligence Meetings specifically directed to targeted crimes such as ATM B&E's, Robberies, Regional Check Frauds or outbreaks of commercial or residential B&Es.
- Daily review of national Crimedex Alerts to ascertain links to other incidents occurring across the country. (ie: Panera Bread Thefts, Felony Lane Gang, and Transient Scams)

MA Crimenet is a listserv that began as a local effort by a few police officers many years ago. A retired DLT from Wilmington Police Dept., J. Chris Neville, who is currently employed as a part-time, 960 employee of the MSP started the eastern MA portion. There was also a

central MA version of this program, which had been run by the former Leicester police chief. After his retirement, this service ceased. (A separate detailed description of MA Crimenet is attached.) Over 4000 emails a year are sent to over 2000 recipients. Intel is shared about organized criminal activity, for example, breaking and entering crews; travelers taking advantage of the elderly; wanted parties or identification needed etc. MA Crimenet also involves organized retail crime investigators and bank investigators. The one individual working on MA Crimenet attends detectives meetings, runs database checks to help solve the information being shared and maintains the listserv all while only being paid for 960 hours a year. He works many more hours than he is paid for, including from other countries while on vacation. Many of the CFC's partners have asked for this service to be expanded to other parts of the state but we currently do not have the bandwidth to handle any more people or information. There are numerous success stories from this listserv each week, often spanning multiple states. With additional personnel, the CFC could expand MA Crimenet to other regions of the state and glean additional intelligence or products from this information. It would give us a better understanding of the smaller, quality of life crimes affecting MA communities. At this point in time, the 960 running MA Crimenet is barely able to keep up with sending emails, let alone, conducting value-added searches, participating in outreach such as detective meetings. In order for MA Crimenet to work and run efficiently, the individuals involved must know about everything being sent or looked at via MA Crimenet. It would not work to have analysts pick up bits and pieces of work related to MA Crimenet if/when time allows. The current staff is extremely busy in their given functions. Currently, MA Crimenet is busiest from mid-morning until 7 or 8 pm. During the early morning, the current employee catches up on information from overnight, and when time allows, reviews crime bulletins, pawn data, information from other intelligence sharing forums and conducts checks of databases to add value. Additional staff on both shifts would allow for all of these functions to be completed as well as bulletins when necessary. Therefore, we request two Intelligence Analyst II's be hired to run MA Crimenet, one on the day shift and one on the eve shift Monday through Friday. Additional personnel would allow us to keep up with the legacy functions of MA Crimentel as well as expand its reach across the Commonwealth and add value by having the analyst produce bulletins when they notice patterns, identify SARs from the MA Crimenet data and funnel information to the correct CFC subject matter expert when appropriate.

Cyber Training Program Coordinator (Vacant/Grant Position)

Duties:

- Assess the instructional or training needs of personnel including CFC Cyber Intel Analysts, Liaison officers/analysts, local, state, federal and private sector partners
- Consult technical, professional, educational and other training personnel through meetings and/or correspondence
- Design curricula and formulate appropriate course content , materials, and terms for Cyber training programs
- Evaluate suitability and effectiveness of Cyber training programs
- Schedule training and awareness seminars and conferences
- Maintain and update training records and files
- Review and write progress reports
- Compile and analyze statistical data and other information for use in research on Cyber training programs, needs assessments
- Perform research and review professional literature
- Attend meetings, conferences, training, and workshops

Education:

- Bachelor's degree in cybersecurity, computer science, computer engineering, information systems, software engineering or a closely related discipline, or an equivalent combination of training, experience, and education including graduate or undergraduate certificates earned at an accredited university or college in computer networking, cloud computing, cyber operations, cybersecurity digital forensics and other cybersecurity related fields

Qualifications:

- Experience working with Cyber Threat Intelligence functions
- Experience working with Incident Response or a Security Operations Center functions
- Understanding of basic threat and vulnerability assessment methodololgies
- Experience creating and implementing cirruculum and lesson plans
- Familiarity with NIST Cybersecurity and MITRE ATT&CK frameworks
- Ability to successfully complete required trainings

Cyber Program Coordinator (Vacant/CIKR Grant Position)

Duties:

- Coordinate and monitor assigned program activities to ensure program effectiveness and compliance with standards, policies, and procedures
- Confer with management staff and other agency personnel to determine program requirements and availability of resources and develop criteria and standards for program evaluation
- Review and analyze data concerning assigned agency programs in order to determine progress and effectiveness, make recommendation for changes and improvements

- Develop and implement procedures and guidelines
- Review reports, intelligence products, memoranda for completeness, accuracy, and content
- Compile and analyze statistical data and other information for use in research on Cybersecurity, Cyber Threat Intelligence, needs assessments
- Respond to inquiries from agency staff and others in order to provide information concerning agency programs
- Provide on-the-job training and orientation for employees
- Liaison and conduct outreach with local, state, federal private sector partners in order to share information and solve problems
- Attend meetings, conferences, training, and workshops
- Review and write progress reports
- Maintain and update records and files

Qualifications:

Education:

- Bachelor's degree in cybersecurity, computer science, computer engineering, information systems, software engineering or a closely related discipline, or an equivalent combination of training, experience, and education including graduate or undergraduate certificates earned at an accredited university or college in computer networking, cloud computing, cyber operations, cybersecurity digital forensics and other cybersecurity related fields

Qualifications:

- Experience working with Cyber Threat Intelligence functions
- Experience working with Incident Response or a Security Operations Center functions
- Experience in project management, handling multiple, concurrent high priority projects
- Understanding of basic threat and vulnerability assessment methodololgies
- Familitiarity with NIST Cybersecurity and MITRE ATT&CK frameworks
- Ability to successfully complete required trainings

MSP & DOT Equipment Collocation Request – Summary for July 2023

History of Request:

LTC Cyr and Sgt. Pack spoke to Joseph Foti and Tony Wade on October 11, 2022 and explained the request, receiving a supportive response.

A follow-up letter was sent by LTC Cyr via email on October 26, 2022. No response was received.

Follow-up calls by Sgt. Pack to Tony Wade have not been productive.

Final call at end of June 2023, Wade informed Sgt. Pack that Foti had told him he had been told that DOT has not historically allowed MSP access to state resources for this purpose and a change in policy would be needed.

Benefit to the Commonwealth:

The Department is working to upgrade and improve its response to AMBER Alert, Silver Alert, kidnapping/abductions, and other public safety and real-time emergency awareness capabilities throughout the Commonwealth. Automatic License Plate Recognition (ALPR) equipment is a critical and indispensable part of this mission. ALPR also supports the Department's homeland security mission, including the investigation and prevention of terrorism and the protection of critical infrastructure and public events such as the Boston Marathon, and the investigation of major crimes and critical incidents. ALPRs alert in real-time when a missing or endangered person is located and can be used to identify vehicles associated with a kidnapping or abduction. There is no other technology or tool that can do that as effectively and efficiently in an emergency.

Why is this Necessary

Currently a child could be abducted in city of Boston and the suspect could drive straight out of Massachusetts along several major highways with absolutely no means of identifying the license plate. Without ALPR, that vehicle's plate may never be identified, and certainly not in a timely manner. According to a 2006 Child Homicide Study conducted by the Washington State Attorney General's Office, which reviewed over 600 child abduction homicides, in 76 percent of the missing children homicide cases studied, the child was dead within three hours of the abduction, and in 88.5 percent of the cases the child was dead within 24 hours.

MSP has identified this as a significant gap in public safety protection in our area of responsibility and is asking for assistance with closing this gap by facilitating the installation of ALPR equipment at a limited number of locations along major highways in the Commonwealth. The locations associated with this request would be selected along major public roadways to provide maximum benefit to the

Commonwealth in emergency situations with negligible privacy implications due to the highly public locations. Additionally, to ensure lawful use and respect privacy considerations, MSP carefully limits and monitor system use, follows all applicable law, and has a thorough and up to date policy on ALPR use.

Request

MSP is asking for DOT to provide access to existing state-owned infrastructure (variable message sign boards and camera poles) on DOT managed highways. No construction or structural modifications are requested. Access to tolling related sites or structures is not requested. We have previously collocated equipment with DOT on the Cape Cod brides since 2014 but have not been assisted with any other locations.

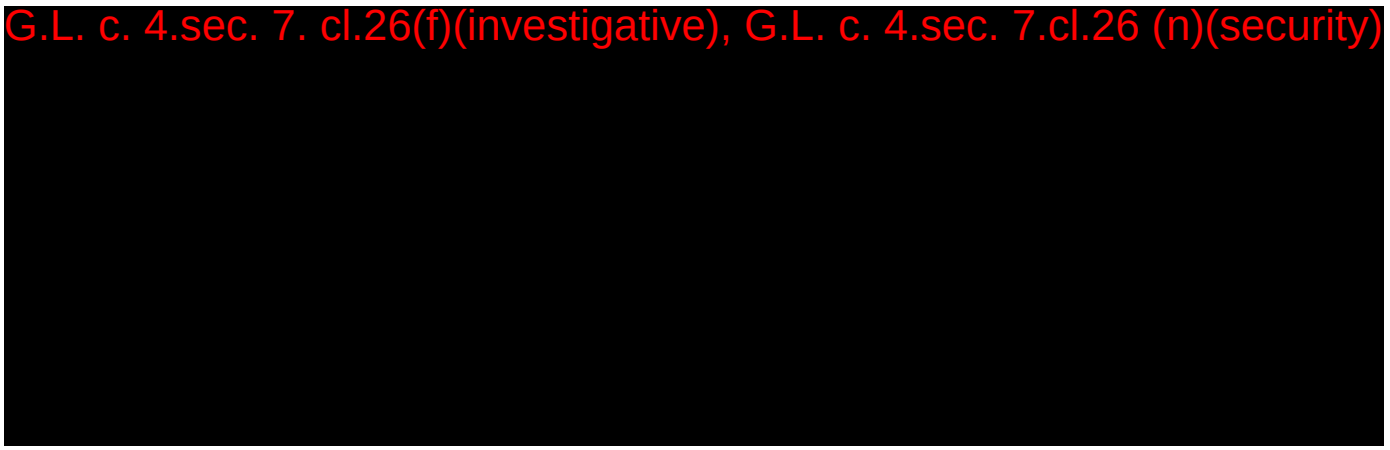
By allowing collocation of equipment, DOT would not assume any financial responsibility, and MSP would continue to be responsible for maintenance and administration. DOT would have no data management access or responsibilities related to our equipment. DOT assistance would be limited to facilitating access to existing power sources and providing instruction on acceptable installation sites and standards. Power draw and equipment weight and footprint are very limited.

MSP has historically had to use solar trailers for highway-based equipment. Solar is a problematic power source, and it has resulted in outages with missed information that could have been important to public safety events. Solar equipment also faces damages from plows and often needs to be removed in winter, rendering the roadways unprotected.

Example of Requested Sites

We have identified the following locations as being critically important to the Commonwealth based on public safety and homeland security factors. Each of these locations has already had MSP equipment deployed currently or in the past along the associated roadway. We have also identified specific DOT sites where we would suggest collocating our equipment.

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



CHARLES D. BAKER
GOVERNOR

KARYN E. POLITO
LIEUTENANT GOVERNOR

TERRENCE M. REIDY
SECRETARY

The Commonwealth of Massachusetts
Department of State Police

Division of Homeland Security and Preparedness
Office of the Division Commander
470 Worcester Road
Framingham, Massachusetts 01702

CHRISTOPHER S. MASON
COLONEL/SUPERINTENDENT

R. SCOTT WARMINGTON
DEPUTY SUPERINTENDENT

October 26, 2022

To: Joseph Foti
Deputy Administrator & Chief of Operations
Massachusetts Department of Transportation, Highway Division

Tony Wade
Director of Statewide Communications and Electronic Systems
Massachusetts Department of Transportation, Highway Division

From: Lieutenant Colonel Mark D. Cyr, #2728
Division of Homeland Security and Preparedness, Division Commander

Subject: MSP & DOT Interagency Equipment Collocation Request

Good morning Mr. Foti and Mr. Wade,

Thank you for taking the time to speak with us on October 11. As we discussed, my division (Homeland Security and Preparedness) is responsible for public safety and homeland security technology projects for the Department of State Police. To that end the Department operates a small number of cameras on highways and major roadways that have the capability of recognizing the license plates of passing vehicles.

This resource is a critical part of the Department's public safety mission and real-time response capability to emergencies in the Commonwealth, including perhaps most importantly to the AMBER Alert and Silver Alert programs. This resource also supports the Department's homeland security mission, including the investigation and prevention of terrorism and the protection of critical infrastructure and public events such as the Boston Marathon.

Except for the Cape Bridges, where we have collocated equipment with DOT since 2014, we use solar power for our highway-based equipment. Solar has proven to be a problematic power source, and it has unfortunately resulted in outages and lost information during critical time periods. As winter approaches this problem is getting worse, and our equipment faces increased outages and damage from weather and plows.

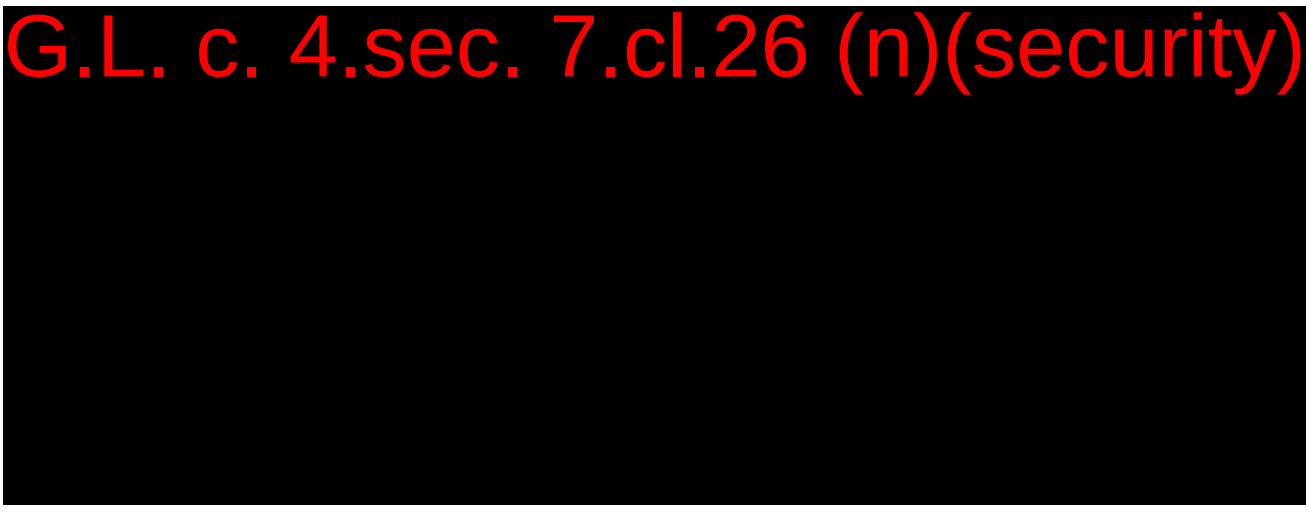
We are working to upgrade equipment that is at or near its end of life, and we are hoping to improve power sources and mounting locations to increase year-round safety and reliability. We are respectfully asking for MassDOT to permit us to collocate equipment on a small number of VMS boards and camera poles that are at or near our existing equipment.

The locations identified herein are associated with pre-existing equipment sites which have been vetted, approved, and carefully selected on major public roadways to provide maximum benefit to the Commonwealth in emergency situations. We do not consider this request to represent an expansion of our system, as we have selected locations along highways where equipment is already in use. Additionally, to ensure lawful use and respect privacy considerations, we carefully limit and monitor system use, follow applicable law, and have a controlling policy.

By collocating our equipment DOT would not assume any financial responsibility for it, and we would continue to be responsible for maintenance, system administration, and data management. We expect that lane closures for installation would be limited and brief, and we would observe any DOT directives regarding timing and traffic control.

We manage and install our equipment and do not subcontract for this purpose. Depending on the site, we may ask for DOT assistance with cable management and accessing/connecting to the on-site power source, but we are not requesting any construction or structural modifications. We have requested (and will provide upon receipt) detailed information on the dimensions and power draw of our equipment. We do not anticipate that either will prove to be a limiting factor.

We have identified the following locations as being critically important to the Commonwealth based on public safety and homeland security factors. Each of these locations has already had MSP equipment deployed along the associated roadway. We have also identified specific DOT ITS sites where we would suggest collocating our equipment. Should any of these specific sites not work, there are other possibilities in each location:



We owe MassDOT a debt of gratitude for the agency's past support and assistance, and we look forward to our continued inter-agency coordination and excellent working relationship. Sgt. Noah

Pack is managing this project for my team and will coordinate with your team on our behalf. Please do not hesitate to reach out to me or him with any questions/concerns.

Respectfully submitted,

Lieutenant Colonel Mark D. Cyr, #2728
Division Commander
Division of Homeland Security and Preparedness

2022 WL 982665
Only the Westlaw citation is currently available.
Supreme Judicial Court of Massachusetts,
Suffolk.

COMMONWEALTH
v.
Jerron PERRY.

SJC-13144
|
Argued December 8, 2021.
|
Decided April 1, 2022.

Synopsis

Background: Defendant was charged with murder in the first degree, attempted masked armed robbery, masked armed robbery, and unlawful possession of a firearm, based on allegations that he robbed multiple convenience stores and gasoline stations at gunpoint and that he shot and killed a store clerk during attempted robbery of one store. Defendant moved to suppress evidence obtained from "tower dumps" of cell site location information (CSLI) for all devices that connected to specific cell towers during a particular time frame. The Superior Court Department, Suffolk County, Robert L. Ullmann, J., denied motion. Defendant filed application in the county court seeking leave to pursue interlocutory appeal. A single justice of the Supreme Judicial Court, Suffolk County, Georges, J., reserved and reported the case to the full court.

Holdings: The Supreme Judicial Court, Gaziano, J., held that:

[1] Commonwealth's use of CSLI, in the aggregate, intruded upon defendant's reasonable expectation of privacy;

[2] first search-warrant affidavit established probable cause to search CSLI from defendant's cell phone;

[3] second search-warrant affidavit failed to establish probable cause to search CSLI from defendant's cell phone;

[4] first warrant described places to be searched and items to be seized with requisite particularity;

[5] only a judge may issue a search warrant for tower dumps of CSLI; and

[6] rule that only judge could issue search warrant for tower dumps of CSLI was "new," and thus applied prospectively.

Affirmed in part, reversed in part, and remanded.

Procedural Posture(s): Appellate Review; Pre-Trial Hearing Motion.

West Headnotes (47)

[1] Criminal Law

Ordinarily, in reviewing a decision on a motion to suppress, an appellate court accepts the judge's subsidiary findings of fact absent clear error but conducts an independent review of the ultimate findings and conclusions of law.

[2] Criminal Law

Where the trial judge's findings concerning a motion to suppress are based exclusively on documentary evidence, an appellate court reviews the judge's findings of fact, as well as his or her conclusions of law, de novo.

[3] Searches and Seizures

The Fourth Amendment to the United States Constitution and the Massachusetts Declaration of Rights protect the right to be free from unreasonable searches. U.S. Const. Amend. 4; Mass. Const. pt. 1, art. 14.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

[4] **Criminal Law**

State constitutional rules do not constrain Federal authorities unless they operate as part of an essentially State investigation.

[5] **Criminal Law**

An investigation is essentially a State investigation, and thus Federal authorities are constrained by State constitutional rules, where, for example, the purpose of the investigation was to bring State charges, State officials retained significant authority over the investigation, or the State's involvement was otherwise so substantial that it negated the essentially Federal nature of the investigation.

[6] **Searches and Seizures**

For the Fourth Amendment's and Massachusetts Declaration of Rights' protections from unreasonable searches to be applicable, the Commonwealth's conduct must constitute a search in the constitutional sense. U.S. Const. Amend. 4; Mass. Const. pt. 1, art. 14.

[7] **Searches and Seizures**

A "search" occurs for purposes of the Fourth Amendment and the Massachusetts Declaration of Rights when the government's conduct intrudes on a person's reasonable expectation of privacy. U.S. Const. Amend. 4; Mass. Const. pt. 1, art. 14.

[8] **Searches and Seizures**

An individual has a "reasonable expectation of privacy" for purposes of the Fourth Amendment and the Massachusetts Declaration of Rights where (1) the individual has manifested a subjective expectation of privacy in the object of the search, and (2) society is willing to recognize that expectation as reasonable. U.S. Const. Amend. 4; Mass. Const. pt. 1, art. 14.

[9] **Searches and Seizures**

In applying the reasonable-expectation-of-privacy test to technological surveillance, courts must be careful to assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted. U.S. Const. Amend. 4.

[10] **Searches and Seizures**

The mosaic theory for determining whether technological surveillance violates a defendant's reasonable expectation of privacy under the Fourth Amendment and the Massachusetts Declaration of Rights requires that courts consider the governmental action as a whole and evaluate the collected data when aggregated. U.S. Const. Amend. 4; Mass. Const. pt. 1, art. 14.

[11] **Searches and Seizures**

Because the whole reveals far more than the sum of the parts, a series of acts may be a search

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

under the mosaic theory for determining whether technological surveillance violates a defendant's reasonable expectation of privacy under the Fourth Amendment and the Massachusetts Declaration of Rights, even where each step in isolation is not. U.S. Const. Amend. 4; Mass. Const. pt. 1, art. 14.

[12] Searches and Seizures

Whether technological surveillance reveals the whole of a defendant's movements, and thus constitutes a search under the mosaic theory, turns on the duration of the surveillance, as well as its degree of comprehensiveness. U.S. Const. Amend. 4; Mass. Const. pt. 1, art. 14.

[13] Searches and Seizures

Long-term technological surveillance raises particular concerns about whether the surveillance constitutes a search under the mosaic theory because it uncovers types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble, thus providing an intimate window into a person's life as it existed throughout the duration of the surveillance; such a pattern of activity is far more revealing than details from isolated incidents. U.S. Const. Amend. 4; Mass. Const. pt. 1, art. 14.

[14] Searches and Seizures

A record created through technological surveillance is considered to be "comprehensive," for purposes of determining whether the surveillance constitutes a search under the mosaic theory, if it has sufficiently voluminous and detailed information from which investigators can derive a relatively complete picture of an individual's comings and goings over time, even if there are gaps in the record. U.S. Const. Amend. 4; Mass. Const. pt. 1, art. 14.

[15] Searches and Seizures

Privacy in one's associations, whether political, religious, or simply amicable, plays a crucial role in maintaining democracy, and therefore is protected under the article of the Massachusetts Declaration of Rights establishing freedom from unreasonable searches and seizures. Mass. Const. pt. 1, art. 14.

[16] Searches and Seizures

Where technological surveillance falls short of revealing the whole of an individual's movements, it nonetheless may constitute a search when it reveals highly intimate details that practically would not have been obtainable using traditional surveillance. U.S. Const. Amend. 4; Mass. Const. pt. 1, art. 14.

[17] Searches and Seizures

Commonwealth's use, during investigation of series of robberies and a homicide, of "tower dumps" of cell site location information (CSLI), in the aggregate, intruded upon defendant's reasonable expectation of privacy, where investigators obtained seven tower dumps spanning seven different days over course of slightly more than one month, collection and analysis of tower dumps provided investigators with highly personal and previously unknowable details of defendant's life, and although each

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

tower dump was limited in time to period immediately before and after specific robbery for which CSLI was sought, collective whole of personal and private information obtained would have been impossible to obtain through use of traditional surveillance techniques. U.S. Const. Amend. 4; Mass. Const. pt. 1, art. 14.

[18] Searches and Seizures

The rights secured by the article of the Massachusetts Declaration of Rights establishing freedom from unreasonable searches and seizures are specific to the individual. Mass. Const. pt. 1, art. 14.

[19] Searches and Seizures

In determining whether a search occurred, for purposes of the article of the Massachusetts Declaration of Rights establishing freedom from unreasonable searches and seizures, a court focuses exclusively on the defendant's privacy interests, and cannot consider the privacy interests of others. Mass. Const. pt. 1, art. 14.

[20] Searches and Seizures

The Massachusetts Declaration of Rights requires that all searches and seizures be reasonable. Mass. Const. pt. 1, art. 14.

[21] Searches and Seizures

Searches and seizures conducted outside the scope of a valid warrant are presumed to be unreasonable, and therefore unconstitutional. Mass. Const. pt. 1, art. 14.

[22] Searches and Seizures

To be "reasonable" in the constitutional sense, a search conducted pursuant to a warrant must be supported by probable cause. Mass. Const. pt. 1, art. 14.

[23] Searches and Seizures

To comport with constitutional protections, an affidavit in support of a search warrant for cell site location information (CSLI) must demonstrate probable cause to believe (1) that a particularly described offense has been, is being, or is about to be committed, and (2) that the CSLI being sought will produce evidence of such offense or will aid in the apprehension of a person who the applicant has probable cause to believe has committed, is committing, or is about to commit such offense. Mass. Const. pt. 1, art. 14.

[24] Searches and Seizures

An affidavit in support of a search warrant for cell site location information (CSLI) must show a sufficient nexus between the criminal activity for which probable cause has been established and the physical location of the cell phone recorded by the CSLI. Mass. Const. pt. 1, art. 14.

[25] Searches and Seizures

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

A nexus between criminal activity for which probable cause has been established and the physical location of the cell phone recorded by cell site location information (CSLI) is sufficient to establish probable cause for a search warrant to obtain the CSLI where the information available to police provides a substantial basis for concluding that evidence connected to the crime will be found in the location to be searched. Mass. Const. pt. 1, art. 14.

[26] Searches and Seizures

To establish probable cause to search the contents of a cellular telephone, it is not enough that the object of the search may be found in the place subject to search; rather, the affidavit in support of the search warrant must demonstrate that the items sought will be located in the particular data file to be searched. U.S. Const. Amend. 4; Mass. Const. pt. 1, art. 14.

[27] Searches and Seizures

General statements in a search-warrant affidavit concerning the ubiquity of cellular telephones are insufficient to establish the required nexus between the commission of offenses and the contents of a telephone, as is required to establish probable cause to search the telephone. U.S. Const. Amend. 4; Mass. Const. pt. 1, art. 14.

[28] Searches and Seizures

The more narrow and demanding standard for establishing a nexus between the commission of offenses and the contents of an electronic device, as is required to establish probable cause to search the device, is applicable to searches of cellular telephones and computer-like devices, and not to searches of cell site location information (CSLI); while a search of the contents of a cellular telephone permits police to view vast amounts of sensitive and private data, the same concerns are not present in the context of CSLI, where the cell phone's location, and not its contents, is sought. U.S. Const. Amend. 4; Mass. Const. pt. 1, art. 14.

[29] Searches and Seizures

When seeking a warrant to search cell site location information (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. U.S. Const. Amend. 4; Mass. Const. pt. 1, art. 14.

[30] Searches and Seizures

Search-warrant affidavit submitted by police officer investigating series of robberies established probable cause to search cell site location information (CSLI) from defendant's cell phone by obtaining "tower dumps" for all devices that connected to specific cell towers during particular time frames, where affidavit described several notable similarities between offenses, evidence indicating that suspected coventurer had acted as getaway driver in at least three offenses, and facts suggesting some reason to believe that defendant and coventurer had communicated with one another from a distance, either prior to or after commission of offense, and thus there was probable cause to believe that either defendant's or coventurer's

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

cell phone would have produced CSLI that would appear in tower dumps. U.S. Const. Amend. 4; Mass. Const. pt. 1, art. 14.

[31] **Searches and Seizures**

Search-warrant affidavit submitted by police officer investigating series of robberies failed to establish probable cause to search cell site location information (CSLI) from defendant's cell phone by obtaining "tower dumps" for all devices that connected to specific cell towers during particular time frames, where affidavit did not set forth any particularized information that perpetrator or suspected coventurer owned cell phone or communicated with one another from a distance, and only ground in affidavit upon which to conclude that defendant had possessed or used cell phone to aid in accomplishing crimes was affiant officer's general statement that "it is very common for a person to have a cellular telephone with them at all times." U.S. Const. Amend. 4; Mass. Const. pt. 1, art. 14.

[32] **Searches and Seizures**

Warrant to search cell site location information (CSLI) from defendant's cell phone by obtaining "tower dumps" for all devices that connected to specific cell towers during particular time frames described places to be searched and items to be seized with requisite particularity, although warrant did not identify suspect by name or telephone number, scope of search authorized by warrant, on its face, was not entirely clear, and, if read in isolation, warrant would have permitted investigators to analyze any and all CSLI in tower dumps, where supporting affidavit explained that investigators sought to obtain tower dumps in order to identify commonalities within CSLI, and thus warrant authorized search of only narrow subset of CSLI, for purposes of identifying a common suspect. U.S. Const. Amend. 4; Mass. Const. pt. 1, art. 14.

[33] **Searches and Seizures**

The article of the Massachusetts Declaration of Rights establishing freedom from unreasonable searches and seizures requires that a search warrant describe with particularity the places to be searched and the items to be seized. Mass. Const. pt. 1, art. 14.

[34] **Searches and Seizures**

The requirement that a search warrant describe with particularity the places to be searched and the items to be seized both defines and limits the scope of the search and seizure. Mass. Const. pt. 1, art. 14.

[35] **Searches and Seizures**

The dual purposes of the requirement that a search warrant describe with particularity the places to be searched and the items to be seized are (1) to protect individuals from general searches and (2) to provide the Commonwealth the opportunity to demonstrate, to a reviewing court, that the scope of the officers' authority to search was properly limited. Mass. Const. pt. 1, art. 14.

[36] **Searches and Seizures**

A search warrant must describe the object of the search with enough specificity that investigators can identify, with reasonable certainty, that

which they are authorized to search, thus ensuring that they search only those items for which probable cause exists. Mass. Const. pt. 1, art. 14.

[37] **Searches and Seizures**

The precise degree of particularity required in a search warrant necessarily varies according to the circumstances and the type of items involved. Mass. Const. pt. 1, art. 14.

[38] **Searches and Seizures**

More generality in a search warrant's description of the places to be searched and the items to be seized may be tolerated where a more precise description would be impracticable. Mass. Const. pt. 1, art. 14.

[39] **Searches and Seizures**

A supporting affidavit can remedy a particularity defect in a search warrant where (1) the warrant makes specific reference to the affidavit and (2) the officer who submitted the affidavit in support of the warrant was one of the officers executing the warrant. U.S. Const. Amend. 4; Mass. Const. pt. 1, art. 14.

[40] **Searches and Seizures**

Unlike an arrest warrant, a search warrant need not identify a specific criminal suspect, although frequently it does. U.S. Const. Amend. 4; Mass. Const. pt. 1, art. 14.

[41] **Searches and Seizures**

Search warrants are often employed early in an investigation, perhaps before the identity of any likely criminal and certainly before all the perpetrators are or could be known, and requiring police to identify a presently unknown suspect by name would unreasonably thwart the ability of the police to investigate a crime. U.S. Const. Amend. 4; Mass. Const. pt. 1, art. 14.

[42] **Searches and Seizures**

Under the statute granting the Supreme Judicial Court general superintendence of inferior courts, the Court may impose requirements, by order, rule or opinion, that go beyond constitutional mandates, including those governing the issuance and content of search warrants. Mass. Const. pt. 1, art. 14.

[43] **Searches and Seizures**

Only a judge may issue a search warrant for "tower dumps" of cell site location information (CSLI), and the 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. Mass. Const. pt. 1, art. 14.

[44] **Searches and Seizures**

Constitutional rule of criminal procedure, that

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

only judge could issue search warrant for "tower dumps" of cell site location information (CSLI), was "new," and thus applied prospectively, where no existing statute or prior judicial opinion would have obligated investigators to obtain search warrant before acquiring or analyzing tower dumps. Mass. Const. pt. 1, art. 14.

[45] Criminal Law

The retroactivity of a constitutional rule of criminal procedure turns on whether the rule is "new" or "old."

[46] Criminal Law

A case announces a "new" constitutional rule of criminal procedure, for purposes of determining whether the holding applies retroactively, if the result was not dictated by precedent; a holding is not so dictated unless it would have been apparent to all reasonable jurists.

[47] Criminal Law

New rules of constitutional rules of criminal procedure apply retroactively if the rule is substantive, defining a class of conduct that cannot be deemed criminal, or prohibiting imposition of a type of punishment on a particular class of defendants or establishes a watershed rule of criminal procedure that is implicit in the concept of ordered liberty, implicating the fundamental fairness of the proceeding.

Cellular Telephone. Constitutional Law, Search and seizure, Privacy, Probable cause, Retroactivity of judicial holding. Search and Seizure, Expectation of privacy, Warrant, Affidavit, Probable cause. Privacy. Probable Cause. Practice, Criminal, Motion to suppress, Warrant, Affidavit, Retroactivity of judicial holding. Retroactivity of Judicial Holding.

INDICTMENTS found and returned in the Superior Court Department on July 12, 2019.

A pretrial motion to suppress evidence was heard by Robert L. Ullmann, J.

An application for leave to prosecute an interlocutory appeal was allowed by Georges, J., in the Supreme Judicial Court for the county of Suffolk, and the case was reported by him.

Attorneys and Law Firms

Eric Tennen, Boston, for the defendant.

Cailin M. Campbell, Assistant District Attorney (Jennifer J. Hickman, Assistant District Attorney, also present) for the Commonwealth.

Mason A. Kortz, for Surveillance Technology Oversight Project, amicus curiae, submitted a brief.

Brett Max Kaufman, Ashley Gorski, & Patrick Toomey, of New York, Jennifer Granick, Jennifer Lynch, & Andrew Crocker, of California, Matthew Spurlock, Committee for Public Counsel Services, Matthew R. Segal, Jessie J. Rossman, Jessica J. Lewis, Nathan Freed Wessler, & Joshua M. Daniels, for American Civil Liberties Union & others, amici curiae, submitted a brief.

Present: Budd, C.J., Gaziano, Lowy, Cypher, Kafker, Wendlandt, & Georges, JJ.

Opinion

GAZIANO, J.

***1** As law enforcement capabilities continue to develop in the wake of advancing technology, so too must our constitutional jurisprudence. To this end, we must grapple with the constitutional implications of "tower dumps," a relatively novel law enforcement tool that provides investigators with the cell site location information (CSLI) for all devices that connected to specific cell

towers during a particular time frame.

Here, the Commonwealth obtained search warrants for seven tower dumps,[1] corresponding to the locations of six robberies and an attempted robbery that resulted in a homicide, all of which investigators believed to have been committed by the same individual. After analyzing the information contained in the tower dumps, investigators determined that the defendant had been near the scenes of two of the crimes. The defendant subsequently was charged with the robberies and the homicide, and he moved to suppress all evidence obtained from the tower dumps as the fruits of an unconstitutional search. A Superior Court judge denied the motion, and the defendant filed an application in the county court seeking leave to pursue an interlocutory appeal; the single justice reserved and reported the case to the full court.

[1] As is customary, each single tower dump included information from multiple cell towers operated by different cellular service providers. See discussion, infra.

The defendant argues that the Commonwealth's use of the tower dumps intruded upon his reasonable expectation of privacy, and therefore effectuated a search under the Federal and State Constitutions. He also contends that search warrants for tower dumps are per se unconstitutional because they necessarily lack particularity. In addition, the defendant asserts that, here, the warrants were not supported by probable cause.

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.

Here, the second of the two search warrants was sufficiently particular and supported by probable cause, and therefore the use of the information obtained from it does not offend the Massachusetts Declaration of Rights. The first warrant, however, was not supported by probable cause, and accordingly, any evidence obtained as a result of it must be suppressed.[2]

[2] We acknowledge the amicus briefs submitted by the Surveillance Technology Oversight Project and by the American Civil Liberties Union, the American Civil Liberties Union of Massachusetts, Inc., the Committee for Public Counsel Services, the Electronic Frontier Foundation, and the Massachusetts Association of Criminal Defense Lawyers in support of the defendant.

1. Background. a. CSLI and tower dumps. An overview of the technology at issue is necessary to a discussion of the issues in this case. Cellular telephones "make calls, send text messages and emails, and access the internet by connecting to a set of radio antennas called 'cell sites' " (quotation and citation omitted). United States v. Thorne, 548 F. Supp. 3d 70, 113 (D.D.C. 2021). See Carpenter v. United States, —— U.S. ——, 138 S. Ct. 2206, 2211, 201 L.Ed.2d 507 (2018). To receive cellular service, "a cellular telephone will connect to the cell site which provides the strongest signal, typically, albeit not always, the nearest one." Commonwealth v. Jones, 477 Mass. 307, 313 n.11, 77 N.E.3d 278 (2017). "The typical cell site covers a more-or-less circular geographic area," with "three (or sometimes six) separate antennas pointing in different directions" which divide the site's radius into smaller, wedge-shaped sectors. Carpenter, supra at 2225 (Kennedy, J., dissenting).

***2** Once a cellular telephone connects with a cell site (either to send or receive communications), the site will "generate[ ] a time-stamped record known as [CSLI]."[3] Id. at 2211. Among other information, this record contains the precise location of the cell site, as well the specific sectors that provided service to the cellular telephone. See Commonwealth v. Augustine, 467 Mass. 230, 237-238, 4 N.E.3d 846 (2014), S.C., 470 Mass. 837, 26 N.E.3d 709 and 472 Mass. 448, 35 N.E.3d 688 (2015) (Augustine I). When a cellular telephone establishes a connection with a particular sector of a cell site, it can be inferred that the user was located within that sector's range of service, or "coverage area," at the time of the connection. Commonwealth v. Wilkerson, 486 Mass. 159, 174, 156 N.E.3d 754 (2020). Service providers retain CSLI for their own business purposes, such as finding weak areas of their network, but it also has proved useful to law enforcement in order to approximate an individual's location at a given time. Carpenter, 138 S. Ct. at 2212.

[3] There are two forms of CSLI. See Commonwealth v. Augustine, 467 Mass. 230,

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

238 & n.18, 4 N.E.3d 846 (2014), S.C., 470 Mass. 837, 26 N.E.3d 709 and 472 Mass. 448, 35 N.E.3d 688 (2015) (Augustine I). Telephone call CSLI is generated only when a cellular telephone uses cell service, such as by placing or receiving a call or a text message. Id. at 238, 4 N.E.3d 846. Registration CSLI, by contrast, is created without any action by the user, as cellular telephones "regularly identify themselves to the nearest cell site with the strongest signal, through a process known as 'registration.' " Id. at 238, 4 N.E.3d 846 n.18. Only telephone call CSLI is at issue here.

The precision with which police are able to approximate an individual's location varies significantly. Some CSLI only enables investigators to place an individual within "an area miles in diameter," whereas other CSLI allows investigators to "calculate users' locations with precision that approaches that of GPS.[4]" ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong., at 23, 25 (2010) (testimony of Professor Matt Blaze) (Blaze Testimony I). The degree of precision largely depends on the size of the sector's coverage area and the technology in use. See id. at 25. The size of the coverage area, in turn, depends on the number of nearby cell sites; "[t]he greater the concentration of cell sites, the smaller the coverage area." Carpenter, 138 S. Ct. at 2211. "As cellular telephone use has grown, cellular service providers have responded by adding new cell sites to accommodate additional customers," resulting in increasingly precise CSLI. See Augustine I, 467 Mass. at 239, 4 N.E.3d 846.

4 Global positioning system.

CSLI also is more precise if the cell site uses newer, more advanced technology. In areas such as Boston that use what is referred to as "small cell" technology, CSLI can identify an individual's location precisely, down to the specific floor of a particular building. See State v. Earls, 214 N.J. 564, 578, 70 A.3d 630 (2013), quoting Blaze Testimony I, supra at 25. See also National League of Cities, Small Cell Wireless Technology in Cities, at 8-9 (2018) (discussing Boston's use of small cell technology).[5] This technology is becoming increasingly ubiquitous; "[b]y some estimates, the number of these small-scale cellular base stations equaled or outstripped the number of conventional cells in the [United States] in 2010, and their deployment continues to grow at a very fast rate." ECPA, Part 2: Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, 113th Cong., at 55 (2013) (testimony of Professor Matt Blaze).

5 Available at https://www.nlc.org/wp-content/uploads/2018/08/CS_SmallCell_MAG_FINAL.pdf [https://perma.cc/8CKW-KJZ8].

***3** In conducting a criminal investigation, law enforcement officers may obtain targeted CSLI, which provides a log of every cell site to which an individual cellular telephone has connected within a given time frame, thus enabling investigators retroactively to reconstruct an individual's movements over time. See Augustine I, 467 Mass. at 239, 4 N.E.3d 846. A tower dump, by contrast, provides officers with CSLI from every device that connected to a particular cell site within a specified period; allowing law enforcement to infer that the owners of those devices most likely were present in that site's coverage area during that time. See Carpenter, 138 S. Ct. at 2220 (tower dump is "a download of information on all the devices that connected to a particular cell site during a particular interval"). Tower dumps have proved particularly useful in investigating serial crimes, because they enable investigators to isolate individual devices that were near the scene of multiple offenses. See Owsley, The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance, 16 U. Pa. J. Const. L. 1, 6 (2013).

b. Factual background. On September 22, September 27, September 28, October 4, October 25, and October 31, 2018, clerks at six stores in Boston, Canton, and Cambridge were robbed at gunpoint by an unidentified perpetrator. On October 6, 2018, an unidentified individual shot and killed a store clerk in Boston during an attempted robbery. Almost all of the stores were convenience stores or gasoline stations, and one sold cellular telephones. Because each of the robberies was perpetrated in a comparable manner by a man fitting a similar description, police suspected that the same person had been responsible for all seven incidents. Based on surveillance footage and witness statements, investigators also believed that the perpetrator was at least occasionally assisted by a coventurer who acted as a getaway driver.

Boston police detectives worked together with agents from the Federal Bureau of Investigation (FBI) to identify a suspect. They sought to do so by cross-referencing a series of tower dumps in order to determine if any device had been near the scenes of two or more of the incidents. To this end, on October 26, 2018, an agent with the FBI obtained a search warrant from a Federal magistrate judge, see 18 U.S.C. § 2703, for tower dumps corresponding to the robberies in Boston, Canton, and Cambridge on September 22, September 27, September 28, and October 4, 2018 (first warrant). The first warrant required four service providers with one or more cell sites near the scenes of the robberies to produce the tower dumps. For each date, the tower dump was to include the CSLI for all cellular telephones that had connected to any cell site providing cellular service to the address where the robbery occurred, within a fifteen-minute period surrounding the time of the incident.

On January 30, 2019, a Boston police detective sought and obtained a search warrant from a judge in the Boston Municipal Court, see G. L. c. 276, §§ 1-7, for tower dumps corresponding to the robberies in Boston and Canton on October 25 and October 31, 2018, as well as the attempted robbery and homicide in Boston on October 6, 2018 (second warrant). The application for this second warrant did not reference or otherwise rely upon any evidence obtained from execution of the first warrant. The second warrant required the same four service providers to produce the tower dumps. For each date, the tower dump was to include CSLI for all cellular telephones that had connected to any cell site serving the address where the crime occurred, within a forty-minute period around the time of each incident.

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,[6] 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.

[6] A "unique identifier" is a distinctive series of numbers that cellular service providers use to identify a device or its user. See Citizen Lab of the Munk School of Global Affairs at the University of Toronto, The Many Identifiers in Our Pockets: A Primer on Mobile Privacy and Security (May 13, 2015), https://citizenlab.ca/wp-content/uploads/2015/05/The-ManyIdentifiers-in-Our-Pockets-A-primer-on-mobile-privacy-andsecurity-_reportPDF.pdf [https://perma.cc/55P6-G43X].

***4** Collectively, execution of the search warrants produced information on over 50,000 unique telephone numbers. Investigators then cross-referenced the data from each tower dump in an effort to identify any telephone numbers that appeared in two or more of the tower dumps, and discovered that a particular telephone number appeared in the tower dump corresponding to the homicide on October 6, 2018, as well as the tower dump corresponding to the robbery on October 31, 2018. Investigators determined, by searching a police database, that this number belonged to the defendant.[7] They 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.

[7] Following an unrelated traffic accident, the defendant previously had provided his telephone number to police.

Based on this, investigators identified the defendant as a suspect in six of the incidents, including the homicide.[8] The defendant was indicted on a charge of murder in the first degree, G. L. c. 265, § 1; attempted masked armed robbery, G. L. c. 274, § 6; five counts of masked armed robbery, G. L. c. 265, § 17; and six counts of unlawful possession of a firearm, G. L. c. 269, § 10 (a). He moved to suppress all of the evidence obtained as a result of the tower dumps, on the ground that it was the fruit of an unconstitutional search.

[8] After having obtained the first warrant, but before applying for the second warrant, the Commonwealth decided that it could not "definitively" determine that the perpetrator who

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

carried out the other offenses was responsible for the robbery on September 28, 2018.

Following a nonevidentiary hearing, a Superior Court judge denied the motion. The judge concluded that the defendant had a reasonable expectation of privacy in his CSLI, and therefore had standing to challenge the purported search. Nonetheless, because the search warrants had been supported by probable cause, the judge decided that the CSLI, and the evidence subsequently derived from it, had been obtained lawfully. The judge found that both search warrants were sufficiently particular and limited in scope, and rejected the defendant's argument that they amounted to "overbroad, unparticularized general warrants." The defendant then sought leave to pursue an interlocutory appeal in the county court. A single justice of this court allowed the application and reserved and reported the matter to the full court.

[1] [2]2. Discussion. a. Standard of review. Ordinarily, "[i]n reviewing a decision on a motion to suppress, 'we accept the judge's subsidiary findings of fact absent clear error but conduct an independent review of [the] ultimate findings and conclusions of law" (quotation omitted). Commonwealth v. Ramos, 470 Mass. 740, 742, 25 N.E.3d 849 (2015), quoting Commonwealth v. Colon, 449 Mass. 207, 214, 866 N.E.2d 412, cert. denied, 552 U.S. 1079, 128 S.Ct. 810, 169 L.Ed.2d 611 (2007). Where, as here, the judge's findings are based exclusively on documentary evidence, we review the judge's findings of fact, as well as his or her conclusions of law, de novo. See Commonwealth v. Johnson, 481 Mass. 710, 714, 119 N.E.3d 669, cert. denied, —— U.S. ——, 140 S. Ct. 247, 205 L.Ed.2d 138 (2019).

[3] [4] [5] [6] [7] [8]b. Whether a search occurred. i. Legal standards. The Fourth Amendment to the United States Constitution and art. 14 protect the right to be free from unreasonable searches.[9] See Commonwealth v. Feliz, 486 Mass. 510, 514, 159 N.E.3d 661 (2020). Of course, for those protections to be applicable, "the Commonwealth's conduct must constitute a search in the constitutional sense." See Johnson, 481 Mass. at 715, 119 N.E.3d 669. Such a search occurs "when the government's conduct intrudes on a person's reasonable expectation of privacy."[10] Augustine I, 467 Mass. at 241, 4 N.E.3d 846. "An individual has a reasonable expectation of privacy where (i) the individual has 'manifested a subjective expectation of privacy in the object of the search,' and (ii) 'society is willing to recognize that expectation as reasonable.' " Johnson, supra, quoting Augustine I, supra at 242, 4 N.E.3d 846.

9 State constitutional rules "do[ ] not constrain Federal authorities unless they operate as part of an 'essentially' State investigation." Commonwealth v. Brown, 456 Mass. 708, 713, 925 N.E.2d 845 (2010), S.C., 466 Mass. 1007, 995 N.E.2d 1091 (2013). An investigation is essentially a State investigation where, for example, the purpose of the investigation was to bring State charges, State officials retained significant authority over the investigation, or the State's involvement was otherwise so substantial that it "negate[d] the essentially Federal nature of the investigation." Commonwealth v. Gonzalez, 426 Mass. 313, 317-318, 688 N.E.2d 455 (1997). The Commonwealth does not dispute that the investigation in this case was essentially a State investigation. Accordingly, the Federal agents involved in the investigation were constrained by the State Constitution. See Commonwealth v. Jarabek, 384 Mass. 293, 297, 424 N.E.2d 491 (1981).

10 Because the defendant does not contend that the government "physically intrud[ed] on a constitutionally protected area," we do not consider whether a physical search occurred. See Commonwealth v. Johnson, 481 Mass. 710, 715, 119 N.E.3d 669, cert. denied, —— U.S. ——, 140 S. Ct. 247, 205 L.Ed.2d 138 (2019), quoting Grady v. North Carolina, 575 U.S. 306, 309, 135 S.Ct. 1368, 191 L.Ed.2d 459 (2015).

***5** [9]In applying this test to technological surveillance, we must be careful to "assure[ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." Carpenter, 138 S. Ct. at 2214, quoting Kyllo v. United States, 533 U.S. 27, 34, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001). In practice, doing so is anything but a simple exercise; 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. See United States v. Jones, 565 U.S. 400, 420, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012) (Alito, J., concurring in the judgment). Thus, while we have "acknowledged the

usefulness of these tools in crime detection," we also have "caution[ed] against allowing the 'power of technology to shrink the realm of guaranteed privacy.' " Commonwealth v. Henley, 488 Mass. 95, 109, 171 N.E.3d 1085 (2021). See Commonwealth v. Blood, 400 Mass. 61, 69, 507 N.E.2d 1029 (1987), quoting Lopez v. United States, 373 U.S. 427, 469, 83 S.Ct. 1381, 10 L.Ed.2d 462 (1963) (Brennan, J., dissenting) ("[i]t must be plain that electronic surveillance imports a peculiarly severe danger to the liberties of the person").

To this end, where police use technology to engage in long-term surveillance, we have analyzed their actions in the aggregate. We first did so with respect to CSLI in Augustine I, 467 Mass. at 253, 4 N.E.3d 846. There, we held that the government effectuated a search when it used targeted CSLI to obtain a list of every cell site to which the defendant's cellular telephone had connected over a two-week period. Id. at 254-255, 4 N.E.3d 846. In so holding, we considered the "cumulative nature of the information collected"; that is, rather than evaluating whether the defendant had a reasonable expectation of privacy in each isolated cell site connection, we evaluated whether the defendant had such a reasonable expectation in the two weeks of CSLI as a whole. Id. at 253-255, 4 N.E.3d 846.

[10] [11]The aggregation principle we used in Augustine I developed into what is now known as the mosaic theory. See Commonwealth v. McCarthy, 484 Mass. 493, 503, 142 N.E.3d 1090 (2020). "The mosaic theory requires that we consider the governmental action as a whole and evaluate the collected data when aggregated." Henley, 488 Mass. at 109, 171 N.E.3d 1085. Thus, rather 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." Kerr, The Mosaic Theory of the Fourth Amendment, 111 Mich. L. Rev. 311, 320 (2012). Because "the whole reveals far more than the sum of the parts," a series of acts may be a search even where each step in isolation is not. McCarthy, supra at 504, 142 N.E.3d 1090. See District of Columbia v. Wesby, —— U.S. ——, 138 S. Ct. 577, 588, 199 L.Ed.2d 453 (2018). "As the analogy goes, the color of a single stone depicts little, but by stepping back one can see a complete mosaic." McCarthy, supra. See United States v. Tuggle, 4 F.4th 505, 517 (7th Cir. 2021), cert. denied, —— U.S. ——, 142 S. Ct. 1107, —— L.Ed.2d —— (2022), quoting Kugler & Strahilevitz, Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory, 2015 Sup. Ct. Rev. 205, 205 (2015) ("the mosaic theory attempts to capture the idea that the 'government can learn more from a given slice of information if it can put that information in the context of a broader pattern, a mosaic' ").

In determining whether a series of acts constitutes 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." Commonwealth v. Mora, 485 Mass. 360, 373, 150 N.E.3d 297 (2020). See Carpenter, 138 S. Ct. at 2217-2218 ("Mapping a cell phone's location [using targeted CSLI] over the course of 127 days" constituted search because it revealed "an intimate window into a person's life" that could not be obtained using traditional surveillance); United States v. Wilford, 961 F. Supp. 2d 740, 771 (D. Md. 2013), aff'd, 689 Fed. Appx. 727 (4th Cir. 2017), cert. denied, —— U.S. ——, 138 S. Ct. 2707, 201 L.Ed.2d 1100 (2018), quoting United States v. Graham, 846 F. Supp. 2d 384, 401-403 (D. Md. 2012), aff'd, 824 F.3d 421 (4th Cir. 2016), cert. denied, 138 S. Ct. 2700 (2018) (mosaic theory turns on whether "discrete acts of surveillance ... in the aggregate ... 'paint an "intimate picture" ' of a defendant's life").

***6** 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. See Henley, 488 Mass. at 113, 171 N.E.3d 1085; Mora, 485 Mass. at 373-374, 150 N.E.3d 297; McCarthy, 484 Mass. at 506, 508-509, 142 N.E.3d 1090; Augustine I, 467 Mass. at 248, 253, 4 N.E.3d 846. The same concerns have animated the Federal cases that have addressed the issue. See Carpenter, 138 S. Ct. at 2217-2218 (targeted CSLI provides "an all-encompassing record of the holder's whereabouts" and therefore reveals "an intimate window into a person's life" that could not have been obtained under traditional surveillance). See, e.g., United States v. Trice, 966 F.3d 506, 518 (6th Cir. 2020), cert. denied, —— U.S. ——, 141 S. Ct. 1395, 209 L.Ed.2d 133 (2021), quoting Carpenter, supra (in evaluating duration of surveillance, considering whether it "provided law enforcement with information that was 'otherwise unknowable,' " and "provided an 'intimate window into a person's life' "). See also Leaders of a Beautiful Struggle v. Baltimore Police Dep't, 2 F.4th 330, 342-343

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

(4th Cir. 2021) (electronic aerial surveillance violates reasonable expectation of privacy because it "yield[s] 'a wealth of detail' " that "surpassed ordinary expectations of law enforcement's capacity and provided enough information to deduce details from the whole of individuals' movements" [citation omitted]); State v. Jones, 2017 S.D. 59, ¶¶ 29, 31, 36, 903 N.W.2d 101, cert. denied, —— U.S. ——, 138 S. Ct. 1011, 200 L.Ed.2d 275 (2018) (search occurred where surveillance that "allowed law enforcement to enhance their senses" revealed "the aggregate of all of [the defendant's] coming and going from the home," thus providing investigators with "a mosaic of intimate details of [the defendant's] private life and associations").

[12] [13]Whether surveillance reveals the whole of a defendant's movements turns on the duration of the surveillance, as well as its degree of comprehensiveness. See, e.g., Augustine I, 467 Mass. at 254, 4 N.E.3d 846. Long-term surveillance raises particular concerns because it uncovers "types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble," United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), aff'd, 564 U.S. 1036, 131 S.Ct. 3064, 180 L.Ed.2d 885 (2011), thus providing "an intimate window into a person's life" as it existed throughout the duration of the surveillance, Carpenter, 138 S. Ct. at 2217. Such a pattern of activity is far more revealing than details from isolated incidents. See Mora, 485 Mass. at 375-376, 150 N.E.3d 297. "The difference is not one of degree but of kind, for no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life ...." Maynard, supra. By way of illustration, a single trip to the liquor store reveals little about an individual, but daily trips over the course of a month reveal much more.

[14]A record is considered to be comprehensive if it has sufficiently voluminous and detailed information from which investigators can derive a relatively complete picture of an individual's "comings and goings" over time, even if there are gaps in the record. See Carpenter, 138 S. Ct. at 2219. For example, in Augustine I, 467 Mass. at 254-255, 4 N.E.3d 846, we determined that the defendant had a reasonable expectation of privacy in the whole of his public movements, as revealed by targeted CSLI from a single cellular telephone that had accompanied him during a two-week trip, despite the fact that his location was only revealed when he made or received a telephone call. See Jones, 565 U.S. at 404, 132 S.Ct. 945 (electronic tracking of particular vehicle's location provided investigators with whole of defendant's movements, even though tracking only revealed defendant's location while in vehicle); Leaders of a Beautiful Struggle, 2 F.4th at 342-343 (rejecting argument that "gaps in the data" nullified reasonable expectation of privacy in public movements). Even where a record does not include each and every one of a defendant's movements, "the likelihood a stranger would observe all those movements is not just remote, it is essentially nil. It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work. It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person's hitherto private routine." McCarthy, 484 Mass. at 504, 142 N.E.3d 1090, quoting Maynard, 615 F.3d at 560.

***7** We also have considered the extent to which the surveillance, even if less comprehensive, tended to reveal highly intimate or personal details. See, e.g., Mora, 485 Mass. at 370-372, 150 N.E.3d 297. Because "art. 14 protects against warrantless intrusion into private places," we have expressed particular concern over surveillance that reveals individuals in private settings. See, e.g., Augustine I, 467 Mass. at 253, 4 N.E.3d 846 ("we cannot ignore the probability that, as CSLI becomes more precise, cellular telephone users will be tracked in constitutionally protected areas"). Such surveillance permits investigators to infer whether and when an individual is in constitutionally sensitive areas, such as the home or a place of worship. See Commonwealth v. Yusuf, 488 Mass. 379, 386, 173 N.E.3d 378 (2021), quoting Caniglia v. Strom, —— U.S. ——, 141 S. Ct. 1596, 1599, 209 L.Ed.2d 604 (2021) ("The very core of [the constitutional] guarantee is the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion" [alterations in original]). Once investigators obtain such information, they are able to piece together "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 the pattern of our professional and avocational pursuits.' " McCarthy, 484 Mass. at 504-505, 142 N.E.3d 1090, quoting Commonwealth v. Connolly, 454 Mass. 808, 834, 913 N.E.2d 356 (2009) (Gants, J., concurring), cert. denied, 574 U.S. 1085 (2015).

This information is private and personal even when

anonymized, but it provides a much richer profile of an individual if it is linked to his or her identity. See United States Dep't of State v. Ray, 502 U.S. 164, 176, 112 S.Ct. 541, 116 L.Ed.2d 526 (1991) ("Although disclosure of [certain] personal information constitutes only a de minimis invasion of privacy when the identities of the [individuals] are unknown, the invasion of privacy becomes significant when the personal information is linked to particular [individuals]"). There is, after all, a significant difference between knowing that an anonymized somebody was at a specific political rally and knowing that "John Smith" was at that rally. See Globe Newspaper Co. v. Boston Retirement Bd., 388 Mass. 427, 435 n.14, 446 N.E.2d 1051 (1983) (anonymized information "which did not allow the identification of any individual" was not "of a personal nature").

[15]Providing law enforcement with such personal information is of particular concern because it risks chilling the associational and expressive freedoms that our State and Federal Constitutions strive to protect. See Jones, 565 U.S. at 416, 132 S.Ct. 945 (Sotomayor, J., concurring) ("Awareness that the government may be watching chills associational and expressive freedoms"); United States v. Moore-Bush, 381 F. Supp. 3d 139, 148 (D. Mass. 2019) (long-term surveillance "risks chilling core First Amendment activities"). Privacy in one's associations, whether political, religious, or simply amicable, plays a crucial role in maintaining our democracy, and therefore is protected under art. 14. See, e.g., National Ass'n for the Advancement of Colored People v. Alabama, 357 U.S. 449, 462, 78 S.Ct. 1163, 2 L.Ed.2d 1488 (1958) (recognizing "the vital relationship between freedom to associate and privacy in one's associations"); Blood, 400 Mass. at 69, 507 N.E.2d 1029 (art. 14 protects "the right to be known to others and to know them, and thus to be whole as a free member of a free society").

We also have considered whether the electronic surveillance generated a category or quantity of information that could not have been obtained using traditional law enforcement tools. See, e.g., McCarthy, 484 Mass. at 500, 142 N.E.3d 1090. To this end, we have examined whether the surveillance allowed the government to "track and reconstruct a person's past movements, a category of information that never would be available through the use of traditional law enforcement tools of investigation" (emphasis in original). See Augustine I, 467 Mass. at 254, 4 N.E.3d 846. Even where the surveillance at issue theoretically could have been accomplished using traditional surveillance methods, we have taken into account whether those methods would have been prohibitively expensive or otherwise impracticable. See, e.g., McCarthy, supra at 499-500, 142 N.E.3d 1090, quoting Jones, 565 U.S. at 429, 132 S.Ct. 945 (Alito, J., concurring) ("[I]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken"). Because "[h]umans are imperfect note-takers and not all blessed with photographic memory," traditional surveillance often cannot achieve the same level of volume, detail, and precision as electronic surveillance. Moore-Bush, 381 F. Supp. 3d at 149. Moreover, as it is "unlikely that investigators could ... maintain[ ] in-person observation over the course of multiple months without [their targets] becoming aware of their presence," technological surveillance that proceeds surreptitiously empowers investigators to engage in long-term, secret surveillance that would not otherwise be possible. See Mora, 485 Mass. at 374, 150 N.E.3d 297.

***8** 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. A few examples are illustrative.

In McCarthy, 484 Mass. at 508-509, 142 N.E.3d 1090, for instance, we decided that police did not intrude on a defendant's reasonable expectation of privacy where they used information obtained from four automatic license plate readers (ALPRs),[11] in fixed positions on either side of two bridges, to determine when, over a period of months, a defendant crossed the bridges. We recognized that the ALPRs provided police with surveillance capabilities that exceeded what would have been possible using traditional law enforcement techniques, but nonetheless reasoned that the limited number of ALPRs, 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.' " Id. at 509, 142 N.E.3d 1090, quoting Carpenter, 138 S. Ct. at 2217. We noted, however, that even a limited number of ALPRs located near "constitutionally sensitive locations," such as the home or a place of worship, could intrude upon a reasonable expectation of privacy because they "reveal more of an individual's life

and associations." McCarthy, supra at 506, 142 N.E.3d 1090.

[11] "Automatic license plate readers are cameras combined with software that allows them to identify and 'read' license plates on passing vehicles. When an ALPR identifies a license plate, it records a photograph of the plate, the system's interpretation of the license plate number, and other data, such as the date, time, location, direction of travel, and travel lane." Commonwealth v. McCarthy, 484 Mass. 493, 494, 142 N.E.3d 1090 (2020).

[16]Thus, where surveillance falls short of revealing the whole of an individual's movements, it nonetheless may constitute a search when it reveals highly intimate details that practically would not have been obtainable using traditional surveillance. See Mora, 485 Mass. at 369, 150 N.E.3d 297. In Mora, supra at 375-376, 150 N.E.3d 297, we decided that police had effectuated a search by installing and monitoring two pole cameras pointed at the defendants' residences. The cameras revealed when the defendants were at home, when they received visitors, and who those visitors were, and therefore did not reveal the whole of the defendants' movements. See id. at 371-372, 150 N.E.3d 297. Nonetheless, we concluded that the cameras intruded upon the defendants' reasonable expectations of privacy because the information revealed by the surveillance provided investigators with highly intimate details of the defendants' lives that could not have been obtained using traditional surveillance methods. See id. at 374, 150 N.E.3d 297, quoting Jones, 565 U.S. at 420 n.3, 132 S.Ct. 945 (Alito, J., concurring) ("replicating pole camera surveillance 'would have required either a very large [pole], a very tiny constable, or both' ").

[17]ii. Application. Here, we must determine whether the government's actions with respect to the seven tower dumps, in the aggregate, intruded upon the defendant's reasonable expectation of privacy by providing investigators with otherwise unknowable details of life.[12] We begin by aggregating the several actions investigators took in acquiring and analyzing the defendant's CSLI. See Henley, 488 Mass. at 113, 171 N.E.3d 1085. Investigators first obtained seven tower dumps, spanning 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.

[12] The Commonwealth does not dispute that the defendant manifested a subjective expectation of privacy in his CSLI records. The defendant submitted an affidavit averring that he never affirmatively permitted law enforcement officers to access his CSLI. See Augustine I, 467 Mass. at 255 & n.38, 4 N.E.3d 846 (subjective expectation of privacy was satisfied where defendant averred that he "never permit[ed] the police or other law enforcement officials access to his telephone records"). Accordingly, we focus on the reasonableness of the defendant's subjective expectation.

***9** These actions, viewed in their entirety, provided investigators with information of a highly personal and private nature. Because tower dumps locate individuals when they are in private settings just as easily as when they are in public settings, they have "the potential to track a cellular telephone user's location in constitutionally protected areas." Augustine I, 467 Mass. at 249, 4 N.E.3d 846. Moreover, tower dumps enable investigators to infer the identity of the individual with whom the user of a particular device was communicating at the moment the device connected to the cell site, and therefore provide investigators with significant insight into the individual's associations.

An owner's location and associations are tied to his or her telephone number and unique identifier, which, here, were used to discern the defendant's identity and that of his suspected accomplice. Moreover, because investigators obtained seven tower dumps spanning seven distinct dates over the course of more than one month, they also were able to piece together a pattern of behavior, that is, not only where an individual was and with whom he or she associated on one occasion, but also where the individual had been and with whom the individual had associated on multiple different occasions.

The collective whole of this personal and private information would have been impossible to obtain

through the use of traditional surveillance techniques. The government learned the defendant's comings and goings during a period of time before he was a suspect, something that could not have been achieved through visual surveillance. See Augustine I, 467 Mass. at 254, 4 N.E.3d 846. Indeed, the sheer volume of information investigators obtained from the tower dumps would have been impossible to gather using traditional surveillance. See id. There is no historic analogue for the ability effortlessly to compile and document the locations, identities, and associations of tens of thousands of individuals, just in case one might be implicated in a criminal act.[13] Even if such a feat were possible, it certainly would be impossible to execute surreptitiously; yet, here, investigators were able to compile and catalogue the locations of more than 50,000 individuals at varying points over more than one month, without any one of them ever knowing that he or she was the target of police surveillance.

[13] Traffic cameras might provide the closest analogue, insofar as they can reveal the retrospective location of potentially a substantial number of people. Traffic cameras, however, only locate a person in public areas, whereas tower dumps provide information about public and private locations. Moreover, while traffic cameras may reveal an individual's physical features, tower dumps enable investigators to determine a person's precise identity using his or her telephone number or unique identifier.

In light of these factors, and in the totality of the circumstances, the collection and subsequent analysis of the seven tower dumps at issue here provided investigators with highly personal and previously unknowable details of the defendant's life. Accordingly, the Commonwealth's use of the seven tower dumps intruded upon the defendant's reasonable expectation of privacy.

The Commonwealth contends that the government's actions here should not be considered a search because the seven tower dumps only produced, in total, three hours of CSLI. In support of its position, the Commonwealth points to Commonwealth v. Estabrook, 472 Mass. 852, 858, 38 N.E.3d 231 (2015), where the court held that no search takes place when police obtain six or fewer hours of targeted CSLI, giving them a list of each cell site with which an identified cellular telephone has connected during that period. We reasoned that, although government collection and use of targeted CSLI over a longer period of time intrudes upon an individual's reasonable expectation of privacy, location information covering six hours or less is too brief in duration to do so. Id.

***10** [18] [19]While Estabrook, 472 Mass. at 855, 38 N.E.3d 231, involved targeted CSLI, its reasoning also is applicable to tower dumps. Given that tower dumps reveal an individual's locations at discrete moments in time, the individual privacy interests implicated by tower dumps are akin to those implicated by targeted CSLI.[14] Compare McCarthy, 484 Mass. at 509, 142 N.E.3d 1090 (no reasonable expectation of privacy in location of individual's vehicle, as revealed by limited number of cameras in particular public location, at specific point in time), with Commonwealth v. Rousseau, 465 Mass. 372, 382, 990 N.E.2d 543 (2013) (reasonable expectation of privacy in entirety of vehicle's movements over thirty-one days). The court's holding in Estabrook, supra at 858, 38 N.E.3d 231, is inapplicable here; the holding permits a warrantless search of up to six continuous hours of CSLI, where, here, the government obtained small increments of CSLI, each falling on a separate day. 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." See id., quoting Augustine I, 467 Mass. at 254, 4 N.E.3d 846. 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. Whereas the former reveals at most one-quarter of one day's activities, the latter reveals a pattern of activity, which implicates comparatively greater privacy interests. See Mora, 485 Mass. at 375-376, 150 N.E.3d 297. Accordingly, although Estabrook, supra, 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.

[14] The defendant argues that there is a heightened privacy interest in the context of tower dumps because they provide CSLI on "potentially thousands of innocent persons." The rights secured by art. 14, however, "are specific to the individual." Commonwealth v. Delgado-Rivera, 487 Mass. 551, 554, 168 N.E.3d 1083 (2021), cert. denied, —— U.S. ——, 142 S. Ct. 908, —— L.Ed.2d —— (2022). Thus, in

determining whether a search occurred, we focus exclusively on the defendant's privacy interests, and cannot consider the privacy interests of others. See id. at 556, 564, 168 N.E.3d 1083 (defendant could not rely on codefendant's reasonable expectation of privacy in cellular telephone in establishing that search occurred).

c. Whether the Commonwealth's acquisition of the tower dumps was constitutionally infirm. Because the Commonwealth's actions constituted a search, we must determine whether its conduct in effectuating that search was reasonable.

[20] [21] [22] [23] [24] [25]Article 14 "require[s] that all searches and seizures be reasonable." Commonwealth v. Alexis, 481 Mass. 91, 97, 112 N.E.3d 796 (2018). "Searches and seizures conducted outside the scope of a valid warrant are presumed to be unreasonable," and therefore unconstitutional. Commonwealth v. Balicki, 436 Mass. 1, 8, 762 N.E.2d 290 (2002). "To be reasonable in the constitutional sense," a search conducted pursuant to a warrant must be supported by probable cause. Commonwealth v. Neilson, 423 Mass. 75, 77, 666 N.E.2d 984 (1996). To comport with constitutional protections, an affidavit in support of a search warrant for CSLI must demonstrate "probable cause to believe [1] 'that a particularly described offense has been, is being, or is about to be committed, and [2] that [the CSLI being sought] will produce evidence of such offense or will aid in the apprehension of a person who the applicant has probable cause to believe has committed, is committing, or is about to commit such offense' " (alterations in original). Estabrook, 472 Mass. at 870, 38 N.E.3d 231, quoting Augustine I, 467 Mass. at 256, 4 N.E.3d 846. Accordingly, the warrant affidavit must show "a sufficient nexus between the criminal activity for which probable cause has been established and the physical location of the cell phone recorded by the CSLI." Commonwealth v. Hobbs, 482 Mass. 538, 547, 125 N.E.3d 59 (2019). A nexus is sufficient where "the information available to police 'provide[s] a substantial basis for concluding that evidence connected to the crime will be found [in] the [location to be searched].' " See Commonwealth v. Ortiz, 487 Mass. 602, 606, 169 N.E.3d 172 (2021), quoting Commonwealth v. Escalera, 462 Mass. 636, 642, 970 N.E.2d 319 (2012).

i. Probable cause. The defendant argues that the search of the CSLI here was unlawful because neither supporting affidavit established probable cause. Specifically, he maintains that the search warrant affidavits did not demonstrate a nexus between the commission of the offenses and the CSLI to be searched, as the affidavits did not set forth particularized evidence that the perpetrator had used a cellular telephone during the commission of the offenses, or in the periods immediately before or thereafter. Relying on Commonwealth v. Morin, 478 Mass. 415, 426, 85 N.E.3d 949 (2017), the defendant contends that the only statements in the affidavits demonstrating that the perpetrator "possessed a phone during the robberies" were general conclusions about the ubiquity of cellular telephones, which cannot be used to establish probable cause.[15] See id. (in demonstrating existence of probable cause to search contents of cellular telephone, "police may not rely on the general ubiquitous presence of cellular telephones in daily life, or an inference that friends or associates most often communicate by cellular telephone, as a substitute for particularized information that a specific device contains evidence of a crime").

15 The affidavit in support of the second warrant stated that "[s]mart phone/electronic device utilization is one of the most common activities today and the vast majority of American society bring their device [wherever] they go, almost by habit." Similarly, the affidavit in support of the first warrant stated that "it is very common for a person to have a cellular telephone with them at all times, even during and after the commission of a crime."

***11** [26] [27] [28] [29]As the defendant contends, to establish probable cause to search the contents of a cellular telephone, "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 ... the items sought will be located in the particular data file ... to be searched" (emphasis in original). Commonwealth v. Broom, 474 Mass. 486, 496, 52 N.E.3d 81 (2016). General statements concerning the ubiquity of cellular telephones are insufficient to establish the required nexus. See Morin, 478 Mass. at 426, 85 N.E.3d 949. This "more narrow and demanding standard," however, is applicable to searches of cellular telephones and computer-like devices, see Hobbs, 482 Mass. at 547 n.11, 125 N.E.3d 59, quoting Commonwealth v. Holley, 478 Mass. 508, 524, 87 N.E.3d 77 (2017), and not to searches of CSLI. While a search of the contents of a cellular telephone permits police to view "vast amounts of sensitive and private data," the "same

concerns are not present in the context of CSLI, where the cell phone's location, and not its contents, is sought." Hobbs, supra. Thus, 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" (emphasis added), which they would be required to do in order to search its contents. See id. at 546, 125 N.E.3d 59. 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. See id.

Here, it is undisputed that the Commonwealth established probable cause to believe that the offenses described in the warrant had been committed. Accordingly, we consider whether each warrant affidavit established a substantial basis to believe that a search of the requested tower dumps would produce evidence of the crimes under investigation, or would aid in the apprehension of the perpetrator. See Estabrook, 472 Mass. at 870, 38 N.E.3d 231. Because the probable cause analysis is "fact-intensive and [must] be resolved on a case-by-case basis," we review each warrant application separately. See Commonwealth v. Vasquez, 482 Mass. 850, 867, 130 N.E.3d 174 (2019), S.C., 485 Mass. 405, 150 N.E.3d 723 (2020), cert. denied, —— U.S. ——, 141 S. Ct. 2601, 209 L.Ed.2d 735 (2021). We begin with the second warrant, in which the warrant affidavit discussed all of the offenses under investigation in depth, before considering the less-detailed first warrant.[16]

16 The affidavit in support of the second warrant did not rely on any evidence obtained pursuant to the first warrant. Accordingly, suppression of the evidence from the first warrant would have no bearing on the admissibility of the evidence obtained pursuant to the second warrant. See Commonwealth v. Tyree, 455 Mass. 676, 692, 919 N.E.2d 660 (2010).

[30]A. Second warrant. The second search warrant affidavit described several notable similarities between the offenses. Each robbery, as well as the attempted 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, see Escalera, 462 Mass. at 642, 970 N.E.2d 319, that the same individual had committed all of the offenses, see Commonwealth v. Marrero, 427 Mass. 65, 71-72, 691 N.E.2d 918 (1998), quoting Commonwealth v. Cordle, 404 Mass. 733, 740, 537 N.E.2d 130 (1989), S.C., 412 Mass. 172, 587 N.E.2d 1372 (1992) ("Although the circumstances of the ... offenses were not identical, we think they were sufficiently similar to justify the inference that they were the product of the same mind" [alterations in original]).

The second warrant affidavit also described evidence indicating that a suspected coventurer had acted as a getaway driver in at least three of the offenses under investigation. The robberies took place from two to eleven miles apart, and some of the locations were not near any public transportation. On October 4, 2018, 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, 2018, a surveillance camera recorded video footage of a dark-colored sedan or coupe traveling at a high rate of speed along the perpetrator's path of flight, as recorded by a separate surveillance camera. Moreover, on October 31, 2018, 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. See Wilkerson, 486 Mass. at 172, 156 N.E.3d 754 (considering existence of and coordination with coventurer in finding probable cause to obtain CSLI).

***12** The search warrant affidavit also described facts suggesting some reason to believe that the defendant and a 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. See Holley, 478 Mass. at 522, 87 N.E.3d 77 (statement that particular crime often involves coordination among codefendants by cellular telephone was considered as one factor in probable cause analysis). This coordination could have taken place while the perpetrators were apart; the robber appeared to travel some distance on foot prior to or after most of the robberies, and therefore was at least temporarily separated from the getaway driver. 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. See Commonwealth v. Almonor, 482 Mass. 35, 45, 120 N.E.3d 1183 (2019), quoting Augustine I, 467 Mass. at 245-246, 4 N.E.3d 846 (cellular telephones "exist as 'almost permanent attachments to [their users'] bodies' " and "physically accompany their users everywhere").

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. See Hobbs, 482 Mass. at 546, 125 N.E.3d 59 (location of cellular telephone as recorded by CSLI can be "reasonably expected to be the location of the person possessing the cell phone"). Accordingly, the second warrant affidavit was supported by probable cause.

[31]B. First warrant. The affidavit in support of the first warrant, much like the affidavit in support of the second warrant, outlined significant similarities amongst the offenses then under investigation, and therefore afforded a substantial basis to believe that the offenses had been committed by the same individual. Additionally, the affidavit demonstrated reason to believe that the perpetrator had been, at least occasionally, assisted by a coventurer.

The first warrant affidavit did not, however, set forth any particularized information that the perpetrator or the coventurer owned a cellular telephone or communicated with one another from a distance. Compare Commonwealth v. Louis, 487 Mass. 759, 765, 169 N.E.3d 1173 (2021) (evidence showed that suspect "communicated with another robbery suspect via cell phone on the date of the murder"); Hobbs, 482 Mass. at 547, 125 N.E.3d 59 (affidavit for targeted CSLI must show that "suspect was known to own or use a particular cell phone"). 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." See Commonwealth v. Rossetti, 349 Mass. 626, 632, 211 N.E.2d 658 (1965) (probable cause must be based on particularized facts, not "simply general conclusions"). Therefore, the evidence obtained pursuant to the first warrant must be suppressed. See Commonwealth v. Andre, 484 Mass. 403, 408, 142 N.E.3d 60 (2020).

[32]ii. Particularity.[17] The defendant also argues that the search here was unreasonable because the search warrants themselves lacked particularity, and therefore were unconstitutional general warrants. He maintains that, if the search of the CSLI was a search in the constitutional sense with respect to him, it necessarily follows that everyone whose CSLI was contained in the tower dumps also was searched. This would render the warrants unconstitutional general warrants because they permitted law enforcement to search the CSLI of third parties who merely were present in the vicinities of the offenses being investigated, without any probable cause. In the defendant's view, the only way to ensure that the scope of a search is sufficiently narrow is to require warrants for CSLI to identify the targeted suspect by name or telephone number.

[17] Having concluded that the first warrant was not supported by probable cause, we need not consider whether it lacked particularity.

***13** [33] [34] [35] [36]As the defendant emphasizes, art. 14 "require[s] that a search warrant describe with particularity the places to be searched and the items to be seized." Commonwealth v. Perkins, 478 Mass. 97, 106, 82 N.E.3d 1024 (2017). The particularity requirement "both defines and limits the scope of the search and seizure." Commonwealth v. Pope, 354 Mass. 625, 629, 241 N.E.2d 848 (1968). "The dual purposes of the particularity requirement are '(1) to protect individuals from general searches and (2) to provide the Commonwealth the opportunity to demonstrate, to a reviewing court, that the scope of the officers' authority to search was properly limited.' " Holley, 478 Mass. at 524, 87 N.E.3d 77, quoting Commonwealth v. Valerio, 449 Mass. 562, 566-567, 870 N.E.2d 46 (2007). See Riley

v. California, 573 U.S. 373, 403, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014) (general searches "allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity"). To this end, a warrant must describe the object of the search with enough specificity that investigators can identify, with reasonable certainty, that which they are authorized to search, thus ensuring that they search only those items for which probable cause exists. See Commonwealth v. Treadwell, 402 Mass. 355, 359, 522 N.E.2d 943 (1988).

[37] [38]The precise degree of particularity required "necessarily var[ies] according to the circumstances and the type of items involved." See Commonwealth v. Freiberg, 405 Mass. 282, 298, 540 N.E.2d 1289, cert. denied, 493 U.S. 940, 110 S.Ct. 338, 107 L.Ed.2d 327 (1989), quoting United States v. Johnson, 541 F.2d 1311, 1314 (8th Cir. 1976). More generality may be tolerated where a more precise description would be impracticable. See, e.g., Henley, 488 Mass. at 119, 171 N.E.3d 1085 (warrant for search of contents of cellular telephone need not particularly identify specific electronic file to be searched "where officers had no knowledge of where on the cell phone evidence might be located, or in what format, but specifically identified the type of evidence sought"); Commonwealth v. McDermott, 448 Mass. 750, 775, 864 N.E.2d 471, cert. denied, 552 U.S. 910, 128 S.Ct. 257, 169 L.Ed.2d 188 (2007) (warrant permitting search of computer files relating to defendant's mental health did not lack particularity because "[t]he lack of further specificity was practical in the circumstances, and the mental health category was limited as much as possible in the circumstances").

We do not agree that all of the individuals whose CSLI was revealed by the tower dumps were subjected to a search in the constitutional sense. 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. See Henley, 488 Mass. at 109, 171 N.E.3d 1085 (search inquiry under mosaic theory focuses on "the governmental action as a whole"). See also Kerr, supra at 320 (search occurs where government "collection and subsequent analysis" of data reveals mosaic [emphasis added]). A cursory examination of anonymized CSLI would not permit investigators to infer the identity of any given individual, where within the cell site's radius that person had been, or with whom he or she had associated; thus, such an examination would not intrude upon a reasonable expectation of privacy. See Andresen v. Maryland, 427 U.S. 463, 482 n.11, 96 S.Ct. 2737, 49 L.Ed.2d 627 (1976); McCarthy, 484 Mass. at 504, 142 N.E.3d 1090. 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.

As the defendant maintains, the scope of the search authorized by the warrant, on its face, is not entirely clear. Under "property to be searched," the warrant lists the "records and information associated with the cellular telephone towers/sites ('Cell Towers/Sites') that provided cellular service" in the vicinity of the crimes during the forty-minute period surrounding each offense. With respect to "particular items to be seized," the warrant identifies the categories of information that the service provider must disclose, including, inter alia, the telephone number of the connecting cellular telephone and the sector of the cell site providing service to each connecting telephone. Thus, if read in isolation, the warrant would permit investigators to analyze, without limitation, any and all CSLI in the tower dumps. Investigators 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. Judicial authorization of such "general exploratory rummaging" undoubtedly would violate the particularity requirements of art. 14. See Balicki, 436 Mass. at 7, 762 N.E.2d 290.

***14** [39]Any deficiencies in the warrant itself, however, were remedied by the supporting affidavit, which adequately limited the scope of the search.[18] See Commonwealth v. Dorelas, 473 Mass. 496, 499 n.3, 43 N.E.3d 306 (2016) (although warrant lacked particularity on its face, search was permissible because affidavit limited scope of search). The supporting affidavit explained that investigators sought to obtain the tower dumps in order "to identify and/or verify commonalities within [the] requested records." Thus, police were permitted to isolate and analyze the CSLI of those telephone numbers that appeared in two or more tower dumps, but no others. 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.[19]

[18] A supporting affidavit can remedy a particularity defect in a warrant where (1) the warrant makes "specific reference to the affidavit" and (2) the officer who submitted the affidavit in support of the warrant was "one of the [officers] executing the warrant." See Commonwealth v. Todisco, 363 Mass. 445, 450, 294 N.E.2d 860 (1973). See also E.B. Cypher, Criminal Practice and Procedure § 5:101 (4th ed. 2021).

[19] The scope of the search was further limited because the warrant permitted investigators to obtain data only for brief periods of time (measured in minutes) surrounding the commission of the offenses. See Commonwealth v. Hobbs, 482 Mass. 538, 546, 549, 125 N.E.3d 59 (2019) (duration of search of targeted CSLI must be limited to period of time bearing sufficient nexus to crime under investigation); Commonwealth v. Dorelas, 473 Mass. 496, 503, 43 N.E.3d 306 (2016) (search of electronically stored information must be limited to electronic files where evidence of crime "may reasonably be found").

[40] [41]As the scope of the search was limited in this manner, that the warrant did not identify a suspect by name or telephone number did not render it insufficiently particular. Unlike an arrest warrant, a search warrant "need not identify a specific criminal suspect -- although frequently it does." Commonwealth v. Martinez, 476 Mass. 410, 419, 71 N.E.3d 105 (2017). See Commonwealth v. Mora, 477 Mass. 399, 404, 77 N.E.3d 298 (2017) ("it is not necessary for the [warrant] application to identify a suspect"). "[S]earch warrants are often employed early in an investigation, perhaps before the identity of any likely criminal and certainly before all the perpetrators are or could be known." Zurcher v. Stanford Daily, 436 U.S. 547, 561, 98 S.Ct. 1970, 56 L.Ed.2d 525 (1978). Requiring police to identify a presently unknown suspect by name "would unreasonably thwart the ability of the police to investigate a crime." See Freiberg, 405 Mass. at 299, 540 N.E.2d 1289. 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. Compare id. at 299-300, 540 N.E.2d 1289 (warrant permitting seizure of "instrument[s] used in crime" was sufficiently particular because "the exact characteristics of [the instruments] were not known to [police]" and warrant affidavit "made it reasonably clear that the 'instrumentalities' sought were related to a crime of violence"), with Commonwealth v. Taylor, 383 Mass. 272, 276, 418 N.E.2d 1226 (1981) (warrant was not sufficiently particular where "the particularization was available but was not used in the warrant").

[42]c. Prospective limits on tower dump warrants. General Laws c. 211, § 3, grants this court "general superintendence of the administration of all courts of inferior jurisdiction." Under this authority, we may "impose requirements (by order, rule or opinion) that go beyond constitutional mandates," Commonwealth v. O'Brien, 432 Mass. 578, 584, 736 N.E.2d 841 (2000), quoting Commonwealth v. Bastarache, 382 Mass. 86, 102, 414 N.E.2d 984 (1980), including those governing the issuance and content of warrants, see, e.g., Preventive Med. Assocs., Inc. v. Commonwealth, 465 Mass. 810, 821-822, 992 N.E.2d 257 (2013); Rodriques v. Furtado, 410 Mass. 878, 888, 575 N.E.2d 1124 (1991). Although this power "is to be used sparingly," it appropriately may be exercised "in exceptional circumstances and where necessary to protect substantive rights in the absence of an alternative, effective remedy" (citation omitted). MacDougall v. Commonwealth, 447 Mass. 505, 510, 852 N.E.2d 1080 (2006).

***15** While the decision we reach today is grounded in individual rights protected by art. 14, we recognize the potential invasions of privacy that could befall those innocent and uninvolved third parties whose CSLI is revealed once an application for a search warrant is allowed. See generally Owsley, supra at 44. Unlike defendants in criminal cases, these individuals may never know that their CSLI was provided to law enforcement, let alone be able to exercise any sort of control or oversight over how their data is used. See id. at 46. Such a situation presents far too great a risk of unwarranted invasions of privacy, whether intentional or inadvertent, malicious or innocent. Cf. Preventive Med. Assocs., Inc., 465 Mass. at 821-822, 992 N.E.2d 257 (exercise of superintendence power was warranted given risk of irreparable invasion of privacy).

[43]Accordingly, in all future cases, only a judge may issue a search warrant for tower dumps. See id. at 822, 992 N.E.2d 257 ("as an exercise of our supervisory powers, we shall require in all future cases that only a Superior Court judge may issue a search warrant seeking e-mails of a criminal defendant under indictment"); Rodriques,

410 Mass. at 888, 575 N.E.2d 1124 ("under the exercise of our general superintendence powers, we shall deem a warrant authorizing the search of a body cavity to be invalid unless issued by the authority of a judge"); G. L. c. 272, § 99 F 1 ("warrant to intercept wire or oral communications" must be issued by Superior Court judge).

The 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. See Matter of the Application of the U.S.A. for an Order Pursuant to 18 U.S.C. §§ 2703(c) & 2703(d) Directing AT&T, Sprint/Nextel, T-Mobile, Metro PCS & Verizon Wireless to Disclose Cell Tower Log Info., 42 F. Supp. 3d 511, 519 (S.D.N.Y. 2014) (warrant application for tower dump must "outline[ ] a protocol to address how the Government will handle the private information of innocent third-parties whose data is retrieved"); Matters of the Search of Cellular Tel. Towers, 945 F. Supp. 2d 769, 771 (S.D. Tex. 2013) ("the Government is ordered to return any and all original records and copies ... to the Provider, which are determined to be not relevant to the Investigative Agency's investigation"); Matter of the Application of the U.S.A. for an Order Pursuant to 18 U.S.C. § 2703(d) Directing Providers to Provide Historical Cell Site Locations Records, 930 F. Supp. 2d 698, 702 (S.D. Tex. 2012) (warrant for tower dump must include protocol for handling of "data related to innocent people who are not the target of the criminal investigation"). See also G. L. c. 276, § 3 ("all property seized [pursuant to a search warrant] shall be restored to the owners thereof" "[a]s soon as may be").

[44] [45] [46]d. Retroactivity. Because we are announcing a constitutionally mandated requirement for the first time, we also must consider whether our holding is to be applied retroactively. The retroactivity of a constitutional rule of criminal procedure turns on whether the rule is "new" or "old." Commonwealth v. Ashford, 486 Mass. 450, 457, 159 N.E.3d 125 (2020). "[A] case announces a new rule if the result was not dictated by precedent" (emphasis in original). Commonwealth v. Bray, 407 Mass. 296, 301, 553 N.E.2d 538 (1990), quoting Teague v. Lane, 489 U.S. 288, 301, 109 S.Ct. 1060, 103 L.Ed.2d 334 (1989). "[A] holding is not so dictated ... unless it would have been 'apparent to all reasonable jurists.' " Chaidez v. United States, 568 U.S. 342, 347, 133 S.Ct. 1103, 185 L.Ed.2d 149 (2013), quoting Lambrix v. Singletary, 520 U.S. 518, 527-528, 117 S.Ct. 1517, 137 L.Ed.2d 771 (1997).

[47]The rule we announce today undoubtedly is new; we are unaware of any existing statute or prior judicial opinion that would have obligated investigators to obtain a search warrant before acquiring or analyzing tower dumps. See Augustine I, 467 Mass. at 257, 4 N.E.3d 846. Accordingly, 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.[20] See Diatchenko v. District Attorney for the Suffolk Dist., 466 Mass. 655, 664, 1 N.E.3d 270 (2013), S.C., 471 Mass. 12, 27 N.E.3d 349 (2015).

20 New rules apply retroactively if the rule "is 'substantive,' defining a class of conduct that cannot be deemed criminal, or prohibiting imposition of a type of punishment on a particular class of defendants" or "establishes a 'watershed' rule of criminal procedure that is 'implicit in the concept of ordered liberty,' implicating the fundamental fairness of the proceeding." Augustine I, 467 Mass. at 257 n.39, 4 N.E.3d 846, quoting Diatchenko v. District Attorney for the Suffolk Dist., 466 Mass. 655, 665, 1 N.E.3d 270 (2013), S.C., 471 Mass. 12, 27 N.E.3d 349 (2015).

***16** 3. Conclusion. The Commonwealth's actions in this case intruded upon the defendant's reasonable expectation of privacy and therefore effectuated a search under art. 14. Nonetheless, because the second warrant was sufficiently particular and supported by probable cause, the evidence obtained pursuant to the second warrant need not be suppressed. All evidence stemming from the tower dumps provided pursuant to the first warrant, however, must be suppressed because the warrant was not supported by probable cause. Our decision is prospective, and also applies to those cases that are active or pending on direct review on the date of issuance of the rescript in this case. Henceforth, 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.

So ordered.

All Citations

--- N.E.3d ----, 2022 WL 982665

End of Document

© 2022 Thomson Reuters. No claim to original U.S. Government Works.

MAURA T. HEALEY
GOVERNOR

KIMBERLEY DRISCOLL
LIEUTENANT GOVERNOR

TERRENCE M. REIDY
SECRETARY

The Commonwealth of Massachusetts
Department of State Police

Division of Homeland Security and Preparedness
Technical Services Unit
21 Oak Street
Leominster, MA 01453

JOHN E. MAWN JR.
COLONEL/SUPERINTENDENT

JOHN D. PINKHAM
DEPUTY SUPERINTENDENT

July 12, 2023

To: Lieutenant Colonel John D. Pinkham, #2772, Deputy Superintendent
Lieutenant Colonel Mark D. Cyr, #2728, Division Commander, DHS
Major Jimi Grasso, #2529, Deputy Division Commander, DHS
Detective Captain John B. Nunes, #2426, Executive Officer

From: Lieutenant Michael A George #2998, Technical Services Unit Commander

Subject: TSU Posting for (1) Sergeant – ALPR Administrator – Interview & Selection

1. On June 22, 2023, Human Resources posted an opening on Power DMS for one (1) Sergeant to serve in the Technical Services Unit within the Division of Homeland Security & Preparedness for the position of Supervisor & ALPR Administrator. Any interested Sergeant was required to submit a To/From and resume to Human Resources and Detective Captain John Nunes, no later than 1700 hours on Monday, July 3rd, 2023. The following two Department members, listed by preference, applied, and were interviewed for the TSU posting om 7/11/23:

Sergeant Ryan M Walczak #3731, State Police Millbury
Sergeant Jason R Macomber #3307, Commercial Driver Licensing

All candidates were interviewed by Major Jimi Grasso, Detective Captain John Nunes and I at GHQ. Lt Colonel Mark Cyr was also present during the interviews. Each candidate was presented with the following standardized questions:

1. Please explain why you applied to be the ALPR Coordinator of the TSU and describe your understanding of the TSU
2. Please explain additional experiences, qualifications, and/or any skill set you feel would be important to the position of TSU/ALPR coordinator.
3. Can you summarize MSP Policy TRF-11 “ALPR”
4. The ALPR Administrator is responsible for training, supervision, and ALPR program management. Please describe any projects you have initiated or have been assigned from inception to completion.
5. Are you willing to be on-call and available to work on short notice, including nights and weekends? Are you able to provide a multi-year commitment and attend out of state training?
6. We are interviewing several candidates for this position, why are you the candidate we should select.
7. This position requires a candidate with strong interpersonal skills. How would you describe your ability to interact with others inside and outside of the department?
8. Why are you leaving your current position?
9. Where do you see yourself in two years?
10. Do you have any questions for us?

3. At the conclusion of the interviews, Major Grasso, Detective Captain Nunes, and I discussed the candidates and their qualifications. Candidates were evaluated on their resumes and responses to the interview questions to determine who would best fulfill the mission of the Technical Services Unit. The following synopsis of each candidate interview provides details of their suitability to make the most significant contribution to the Technical Services Unit.

4. On Tuesday July 11, 2023, at 1200 hrs D-Capt Nunes and I interviewed Sgt Ryan Walczak at GHQ. Sgt Walczak was attired in a business suit and presented neatly and professionally. His responses were knowledgeable, thoughtful, and articulate. His resume showed extensive investigative experience in specialty units including SERT, CAT teams and the Gang Unit where he participated in wiretap investigations, GPS tracking invests and pole camera operations. His interaction with the interviewers was enthusiastic and left a positive impression. He had a high understanding of the TSU responsibilities, he recited all the key points of the ALPR policy (TRF-11) and case law (CW v McCarthy), has experience in project management in the Gang Unit and has experience creating power point presentations and presenting to MSP Academy and Local PD's while in the Gang Unit.

5. On Tuesday July 11, 2023, at 1235 hrs D-Capt Nunes and I interviewed Sgt Jason Macomber at GHQ. Sgt Macomber was attired in a business suit and presented neatly and professionally. His responses were knowledgeable, thoughtful, and articulate. His resume showed experience in specialty units including CODIS, Dive Team and CDL licensing. His interaction with the interviewers was enthusiastic and left a positive impression. He understood the TSU responsibilities; he recited all the key points of the ALPR policy (TRF-11) and case law (CW v McCarthy). He has experience in project management while in the CODIS Unit and has presented water safety training to the MSP Academy recruits while on the Dive Team.

6. Both candidates interviewed well and proved capable of assuming the ALPR administrator position. To narrow the selection process, I spoke with members of the specialty units both members had recently left (SERT and the Dive Team) as well as members of TSU to gain an understanding of interpersonal relationships and work ethic. Both candidates received good reviews however Sgt Walczak received the highest praise on interpersonal skills, work ethic and unit cohesion. This information was shared with Major Grasso and Detective Captain Nunes.

7. Based on all the factors listed above I respectfully suggest the selection of Sgt Ryan Walczak #3731 for the TSU/ALPR Administrator position.

Respectfully submitted,



Lt Michael A George #2998
Division of Homeland Security and Preparedness
Technical Services Unit
Michael.george@pol.state.ma.us
774-229-6109

Subject: UTILIZATION OF VIDEO SYSTEMS IN THE COMMONWEALTH WATCH CENTER

Policy:

The availability and use of video at the Commonwealth Watch Center provide opportunities for enhancing security for the Commonwealth's infrastructure, major events, government agencies, and coastal maritime and port operations. The use of video systems increases the productivity and effectiveness of law enforcement and public safety agencies and provides opportunities to increase officer and public safety.

It is the policy of the Department of the State Police (Department) to respect the privacy interests of all persons in the Commonwealth. The Watch Center shall only utilize video systems in furtherance of official and legitimate law enforcement operations and public safety or security and shall comply with all applicable laws and Department Policies and Procedures, Rules and Regulations, Fusion Center, and/or unit-specific operating procedures.

Purpose and applicability:

A. Establish guidelines and procedures for the proper use and application of video systems utilized by the Commonwealth Watch Center.

B. To provide guidelines and principles for collecting, accessing, disseminating, and retaining video system recordings, data, and information.

C. To ensure that such recordings, data, and information are used for legitimate law enforcement purposes and that individuals' privacy, civil rights, and civil liberties are not violated.

D. Excluding Cruiser Mounted Cameras and Body Worn Cameras governed by ADM-35 and Automatic License Plate Recognition (ALPR) technology governed by TRF-11, this policy applies to any and all live-feed video systems, with or without video recording capabilities, accessible within the Commonwealth Watch Center, including, but not limited to:

(1) Department Video Systems;

(2) External Video Systems;

(3) Massachusetts Coastal Maritime Security Video System (CMSVS);

(4) MassDOT Highway Cameras; and

(5) Any additional live-feed video systems, with or without video recording capabilities, utilized on a long-term or temporary basis including instances such as covert operations, special events, or demonstration/trial purposes.

Definitions:

Department Video Systems: All video camera systems operated and maintained by the Department with live-feed viewing, with or without video recording capabilities, but not limited to, Department-operated building and infrastructure security camera systems and video cameras operated by the MSP Air Wing with the ability to provide live-feed video or imagery, with or without recording capabilities, through the use of aviation aircraft and unmanned aerial vehicles (UAVs), but excluding Cruiser Mounted Cameras and Body Worn Cameras as governed by ADM-35 and Automatic License Plate Recognition (ALPR) technology as governed by TRF-11

External Video Systems: All video camera systems operated and maintained by agencies, municipalities, or private entities outside of the Department that provide the Commonwealth Watch Center with live-feed video or imagery with or without video recording capabilities.

Live-Feed Video or Imagery: All video or images, digital or analog, streamed or transmitted from a live, not recorded, source.

Grant Provisions: The provisions of the U.S. Department of Homeland Security / Federal Emergency Management Agency Port Security Grant (Sub Account No. EMW-2020-PU-0056) awarded to the Massachusetts Executive Office of Public Safety (EOPSS), effective on July 1, 2022, and any/all subsequent related grants or award(s).

Massachusetts Coastal Maritime Security Video System (CMSVS): A U.S Department of Homeland Security / Federal Emergency Management Agency grant funded, Executive Office of Public Safety and Security secure network of port and maritime security cameras connected to an isolated server designed to be both interoperable with existing Department of Homeland Security Urban Security Initiative and United States Coast Guard camera systems and accessible to participating federal, state, and municipal agencies.

MassDOT Highway Cameras: A Massachusetts Department of Transportation video camera system providing live-feed video or imagery, with or without recording capabilities, of highways, roadways, and other location points throughout the Commonwealth.

Administration & Operation:

A. The Department shall manage, maintain, and oversee all Department video systems. Department equipment, recordings, data, and information shall be acquired, processed, maintained, disseminated, and/or disposed of in accordance with this policy, Department policy, Fusion Center Standard Operating Procedures, grant provisions, and all applicable laws.

B. External video systems shall be managed, maintained, and overseen by the respective agencies and municipalities responsible for such systems. External video

system recordings, data, and information shall be acquired, processed, maintained, disseminated, and/or disposed of in accordance with any applicable agreement with the entity responsible for each external video system as well as this policy, Department policy, Fusion Center Standard Operating Procedures, grant provisions, and all applicable laws.

C. The Department shall, as delegated by the Colonel or a designee and on behalf of and by agreement with EOPSS, manage, maintain, and oversee CMSVS. CMSVS equipment, recordings, data, and information shall be acquired, processed, maintained, disseminated, and/or disposed of in accordance with this policy, Department policy, Fusion Center Standard Operating Procedures, grant provisions, and all applicable laws.

Authorized Access and Uses:

A. Access to video viewable at the Commonwealth Watch Center that are not available to the general public shall be restricted to authorized Watch Center employees, Fusion Center employees, Department employees with Watch Center access, and other individuals authorized by the Commonwealth Watch Center supervisor, Fusion Center Commander, Division Commanders, or the Colonel or designee.

B. Use of video viewable at the Commonwealth Watch Center video are strictly limited to law enforcement and public safety purposes only. The following are valid law enforcement and public safety purposes:

(1) Preventing, monitoring and/or mitigating any threat to infrastructure, government, homeland security, port or coastal security, major events, law enforcement, or public health and safety;

(2) Supporting law enforcement and public safety agencies during major events, critical incident responses, and exigent circumstances;

(3) Criminal investigations;

(4) Crime analysis; and

(5) Criminal intelligence gathering.

C. Watch Center personnel and other authorized users shall not utilize video systems to monitor or gather information about:

(1) Individuals or organizations solely on the basis of their religious, political, social views or activities; or

(2) An individual's or organization's participation in a particular non-criminal organization or lawful event; or

(3) An individual's age, race, ethnicity, religion, citizenship, place of origin, disability, gender, gender identity, genetic information, or sexual orientation unless such information is relevant to the individual's criminal conduct or activity or if required to identify the individual.

Restricted Uses and Limitations:

A. Transmitting or recording audio on a Commonwealth Watch Center video device is strictly prohibited. Due to the possibility of violating legitimate privacy expectations, inadvertently recording protected conversations, or unintentionally violating M.G.L. c. 272, §99 (Interception of Wire and Oral Communications), all Commonwealth Watch center video system devices shall be configured so they do not transmit or record audio unless otherwise permitted by law.

B. Using or requesting the use of Commonwealth Watch Center video for personal use is strictly prohibited and considered employee misconduct as well as a violation of this policy.

C. Commonwealth Watch Center video equipment and technology shall not be intentionally used for viewing, recording, or transmitting images or video in a criminal investigation at any location or property where a person has a reasonable expectation of privacy unless:

(1) A warrant or court order has been approved for the search of the property;

(2) Consent by the owner or person responsible for the property is obtained; or

(3) Exigent circumstances exist, including but not limited to: search and rescue missions, tactical missions, crash/accident scenes, crime scenes, fire scenes, hazmat scenes and/or natural disasters.

Prosecutorial & Court Ordered Restrictions:

Commonwealth Watch Center video data, and information are subject to state and federal laws and any court of competent jurisdiction orders. Video recordings shall be preserved, stored, and retained in accordance with the requests, directions, and orders of appropriate prosecutorial and/or judicial authorities.

Preservation of Video System Data:

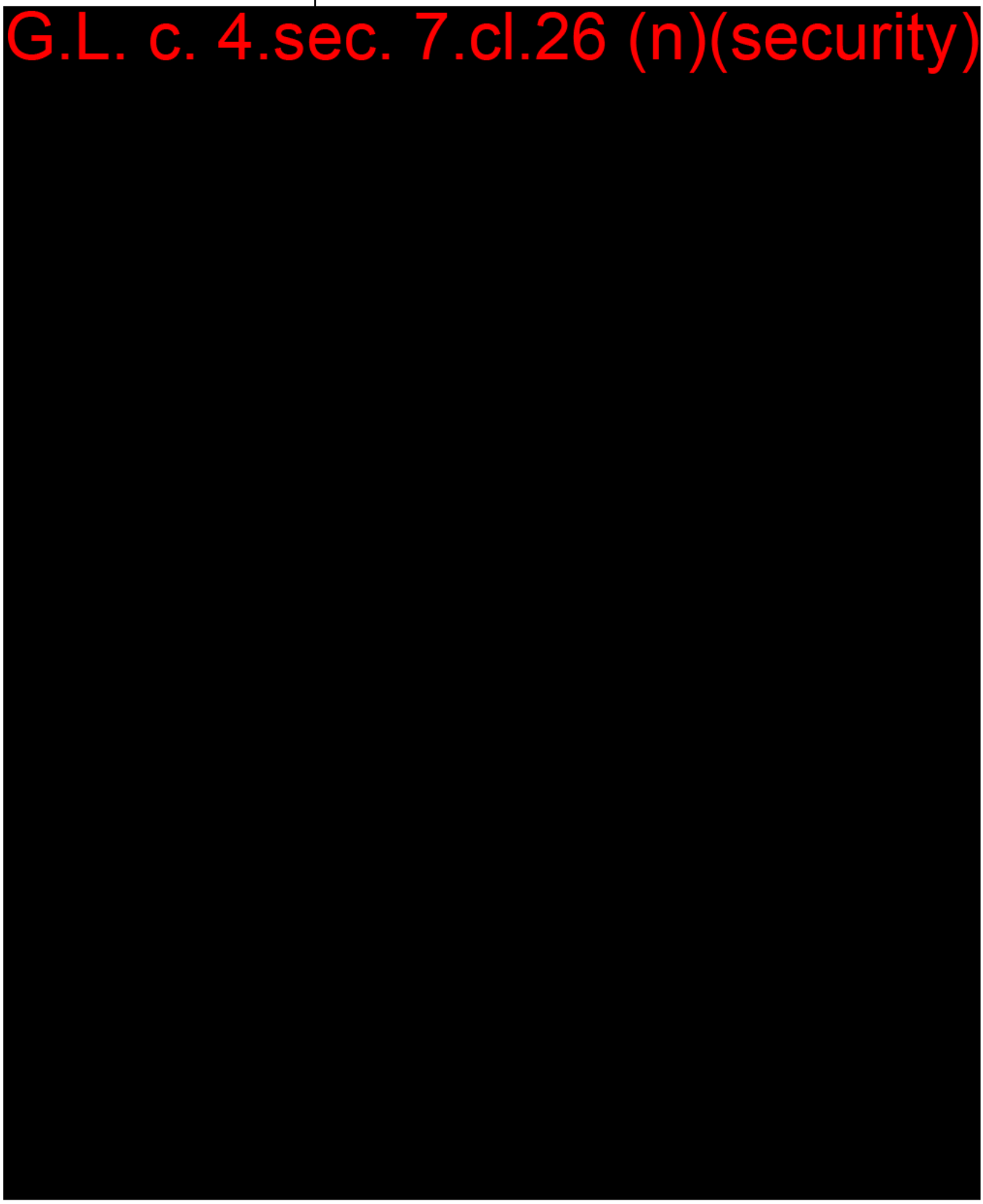
All Commonwealth Watch Center video recordings, data, and information shall be processed, maintained, disseminated, preserved and/or destroyed in accordance with applicable Department and/or Fusion Center policies and procedures, including but not limited to those concerning public records, privacy, and the preservation of evidence.

Commonwealth Fusion Center
Accounts

ORI: MAMSPA800

Cameras

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



Cameras (cont.)

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

[redacted]

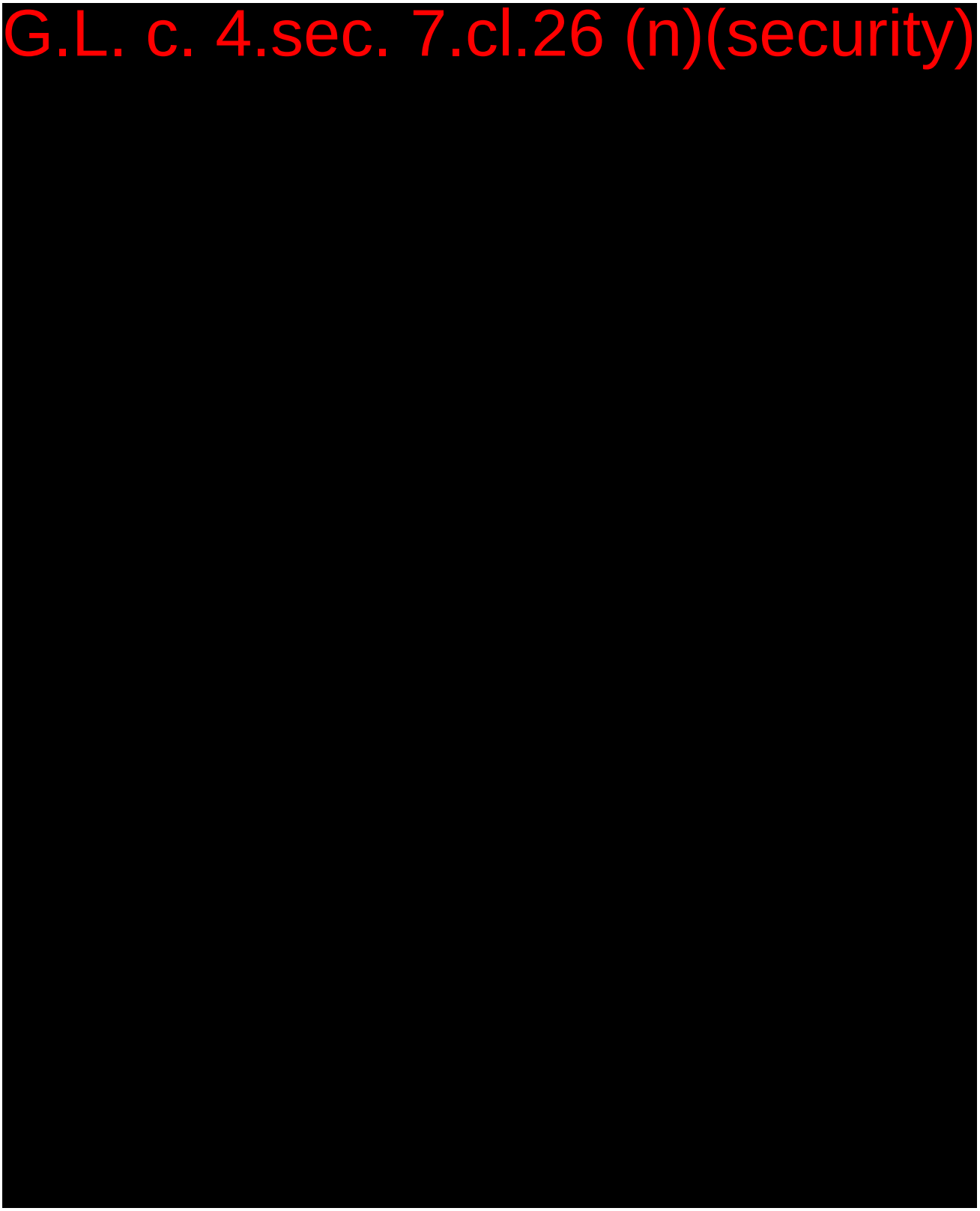
Commonwealth Fusion Center
Accounts

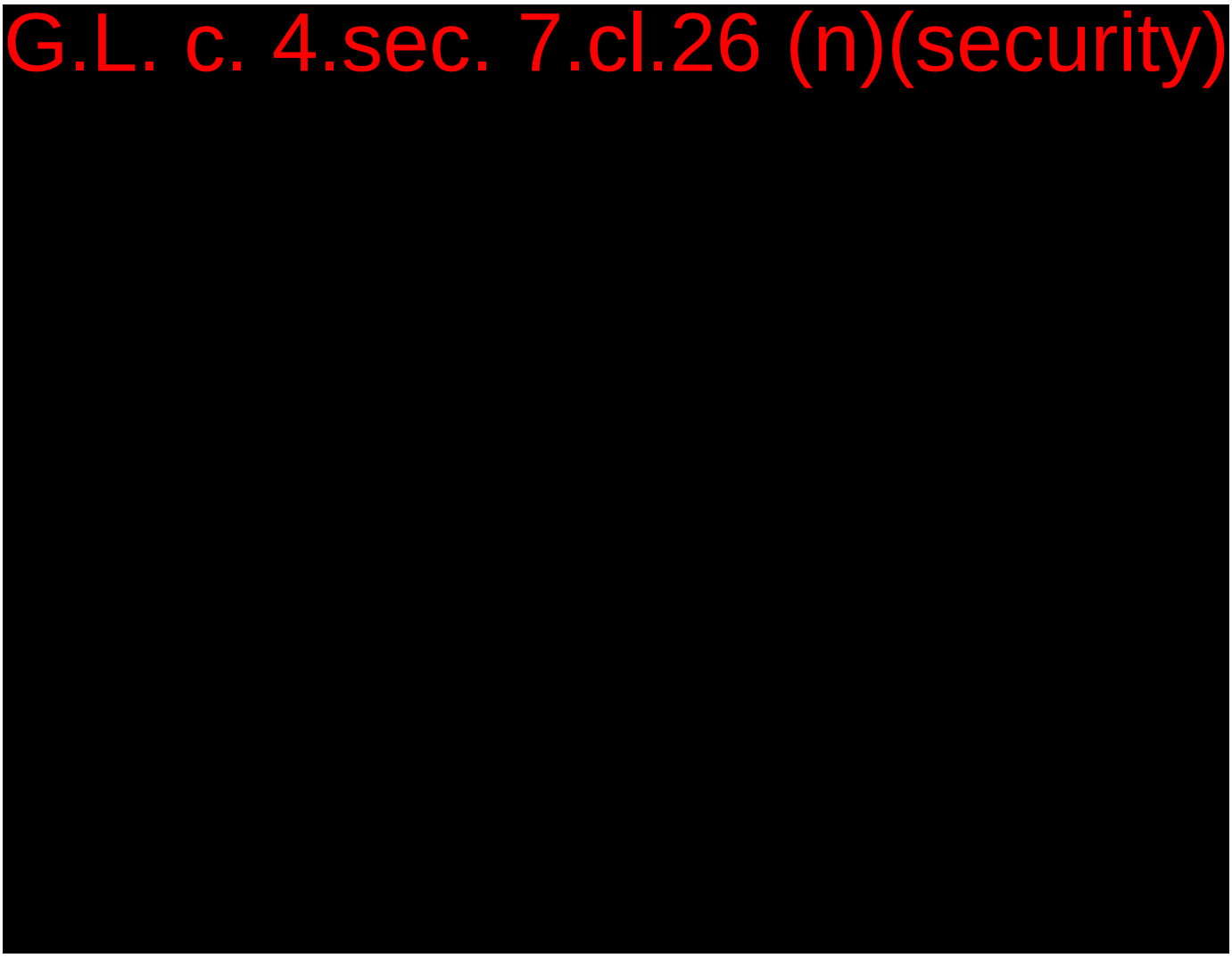
UN: watchcenter **PW:** WatchCenter2020!

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

Miscellaneous

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


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



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.

Commonwealth Fusion Center (CFC)
Massachusetts

(978) 451-3700 | (508) 820-2233

Name					
DOB:					
OLN:		Registered Vehicles:	Yes: ☐	No: ☐	
SSN:					
FBI #:					
SID #:					
BOP:	Yes: ☐	No: ☐	III (QH/QR):	Yes: ☐	No: ☐
WMS:	Yes: ☐	No: ☐	BOPFI/FSI	Yes: ☐	No: ☐

Address 1:		City:		State	
Address 2:		City:		State	
Address 3:		City:		State	

Phone 1:	
Phone 2:	
Phone 3:	

Open Source 1:	
Open Source 2:	
Open Source 3:	

ACISS:	Yes: ☐	No: ☐	Related Case(s):	Yes: ☐	No: ☐	Case #:	
Coplink:	Yes: ☐	No: ☐					
PIX:	Yes: ☐	No: ☐					
AFIS-R:	Yes: ☐	No: ☐					
InmateWeb:	Yes: ☐	No: ☐					
MIDNET:	Yes: ☐	No: ☐					

CLEAR:	Yes: ☐	No: ☐
TLO:	Yes: ☐	No: ☐
ISO:	Yes: ☐	No: ☐

Analyst Notes:

Requester Name:	
Requester Agency:	
Reference #:	

Unclassified//Law Enforcement Sensitive

The information contained herein is Law Enforcement Sensitive and intended For Official Use Only. No portion of this product should be released, copied or reproduced or re-disseminated without prior approval of the Commonwealth Fusion Center.

Department of State Police
DIVISION COMMANDER'S ORDER

Issue Date	**Number**
September X, 2023	**2023-DHS-00X**
Subject: **ALPR Data Retention & Access**	

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 significantly enhances public safety by augmenting the operational and investigative effectiveness of law enforcement agencies.

The use of ALPR technology is governed by General Order TRF-11 "Automatic License Plate Recognition". In addition, the use of ALPR systems shall be subject to the guidelines set forth in this Order unless superseded by General Order TRF-11.

Pursuant to General Order TRF-11, the retention of ALPR data collected by the Department shall be determined by the Department of Criminal Justice Information Services (DCJIS) policy. Furthermore, ALPR systems operated by the Department shall be configured to restrict data visibility for a maximum duration of sixty (60-) days from the date of the initial request.

Users requesting to access records beyond sixty (60) days shall contact the Commonwealth Watch Center, the ALPR Administrator, or other administrator authorized by the Division Commander of Homeland Security and Preparedness. The request will be reviewed on a case-by-case basis. In the absence of exigent circumstances, the user may be required to revise their request, consult with a District Attorney's Office of jurisdiction, or to submit legal process to obtain the requested records.

_____

Mark D. Cyr
Lieutenant Colonel
Division of Homeland Security and Preparedness